Exhibit B

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Warrants for All Content and Other Information Associated with the Email Account [redacted] Maintained at Premises Controlled by Google LLC, and the iCloud Account with [redacted] and Registration Email [redacted] Maintained at Premises Controlled by Apple Inc.,

USAO Reference No. 2020R00816

22 MAG 748

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

Agent Affidavit in Support of Application for Search Warrants for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

MARY JO CORKERY, Special Agent, Federal Bureau of Investigation, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for approximately 21 years. For approximately 7 years, I have been assigned to a public corruption squad in the FBI's New York field office. I have received training regarding electronic evidence and participated in the execution of search warrants involving electronic evidence.

B. The Providers, the Subject Accounts, and the Subject Offenses

2. I make this affidavit in support of an application for search warrants pursuant to 18 U.S.C. § 2703 for all content and other information associated with the following:

SDNY_R_00004189

a. Email account [redacted] ("Subject Account-1"), which is maintained and controlled by Google LLC ("Google"), headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. As set forth below, Subject Account-1 is believed to be used by United States Senator Robert Menendez.

b. The Apple iCloud account with associated [redacted] and registration email [redacted] ("Subject Account-2," and together with Subject Account-1, collectively, the "Subject Accounts"), which is maintained and controlled by Apple Inc. ("Apple," and together with Google, the "Providers"), headquartered at 1 Infinite Loop, Cupertino, California 95014.[1] As set forth below, Subject Account-2 is believed to be used by Senator Robert Menendez.

3. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrants. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and/or instrumentalities of violations of (i) 18 U.S.C. §§ 201 and 371 (bribing or offering to bribe or demanding or accepting a bribe, and conspiring to do the same, with respect to a United States Senator); (ii) 18 U.S.C. §§ 1343, 1346, and 1349 (honest services wire fraud and conspiring to commit honest services wire fraud); (iii) 18 U.S.C. § 1951 (extortion under color of right and conspiring to do the same); and (iv) 18 U.S.C. §§ 1956 and 1957 (money laundering, engaging in a financial transaction in criminally-derived property, and conspiracy to do one or both of the same) (collectively, the "Subject Offenses"). This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the

[1] The registration email account for Subject Account-2 is similar to Subject Account-1, but varies by one character. As noted below (*see* paragraph 46), the recovery email account for Subject Account-1 is the registration email account for Subject Account-2.

limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Providers

4. I have learned the following about Google:

a. Google offers to the public a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications using a username and password. Once logged into a Google account, a user can connect to Google's full suite of services offered to the general public.

b. In particular, as relevant here, Google offers free, web-based email services to the public. Specifically, Google allows subscribers to maintain email accounts through Gmail under the domain gmail.com and other domain names chosen by the user or an enterprise. A subscriber using Google's services can access his or her email account from any computer connected to the Internet.

c. Google maintains the following records and information with respect to every Google account that has email services:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, recovery and alternate email addresses, and sign-in phone numbers. A recovery email address, which can be associated with more than one Gmail account, is used to regain access to an account if a password has been forgotten or a user has been locked out of their account. An alternate email address is a non-Gmail account that a user has provided that can be used to sign into a Gmail account. A sign-in phone number is a phone number that can be used as a primary/additional login identifier to access an account. Google also maintains records concerning the date on which the account was created, the IP address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of Google services utilized by the subscriber. Finally, Google maintains records regarding (1) fetching and forwarding email addresses, which are email accounts from which the primary account receives emails and forwards emails, respectively; (2) email aliases, domain aliases or separate domains associated with the account, which are means by which accounts with other domain names or other email addresses can be associated with a primary Google account; (3) other Google accounts that have access to the primary account, which access can be granted by the user of the primary account; and (4) other email accounts that are associated with the primary Google account.

iii. *Device Information.* Google may also collect and maintain information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers

("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

iv. *Cookie Data.* Google typically uses features to track the activity of users of its accounts, including whether or not the user of an account accesses other accounts at Google using the same computer or device, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

v. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system, including records of login and logout events relating to Google accounts, including user IP addresses and dates and timestamps.

vi. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

vii. *Preserved and backup records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). Google may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

b. Google also maintains records with respect to other Google services, which it stores in connection with a Google account and includes the following:

i. *Google Contacts.* Google provides an address book for Google accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Google preserves contacts indefinitely, unless the user deletes them.

ii. *Google Calendar.* Google provides users with the ability to create and maintain online calendars, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars. Google preserves appointments indefinitely, unless the user deletes them.

iii. *Google Messaging Content.* Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user has not disabled that feature or deleted the messages.

iv. *Google Drive content.* Google Drive is a cloud storage service automatically created for each Google account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage

limit. Google provides users with a certain amount of free storage, currently 15 gigabytes, and users can purchase a storage plan through Google to store additional content. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others and grant those with access the ability to edit or comment. Google maintains a record of who made changes and when to documents edited in Google applications. Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

v. *Google Maps*. Google Maps is service which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. If users log into their Google account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps. Google stores Maps data indefinitely, unless the user deletes it.

vi. *Google Photos*. Google Photos is a cloud-based photo and video storage service through which users can share or receive photos and videos with others. Users have the option to sync their mobile phone or device photos to Google Photos. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google Photos if that data is included by the user as part of the upload. This metadata includes what is known as

exchangeable image file format (or "Exif") data, and can include GPS location information for where a photo or video was taken.

vii. *Location History data*. Google collects and retains data about the location at which Google account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. This location data may be associated with the Google account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google account, such as Location History or Web & App Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

viii. *Chrome Browser and "My Activity" Data*. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google account in a record called My Activity. My Activity also collects and retains data about searches that users conduct within their own Google account or using the Google Internet search engine available at http://www.google.com while logged into their Google account.

5. I have learned the following about Apple:

a. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

b. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

i. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

ii. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

iii. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages

opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

iv. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

v. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

vi. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

vii. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

c. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an

SDNY_R_00004189

Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

d. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

e. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple

SDNY_R_00004189

also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

f. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

g. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and

iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

6. In my training and experience, evidence of who was using an email account, Google account, and/or Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion.

7. For example, the stored communications and files connected to an electronic account, such as the Subject Accounts, may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

8. In addition, the user's stored electronic communications, IP logs, and other data retained by the Providers, can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email content, and stored

documents and photos and videos (and the data associated with the foregoing, such as geo-location, date, and time) may be evidence of who used or controlled the Google account and/or Apple account at a relevant time. Further, the Providers' account activity can show how and when the account was accessed or used. For example, as described herein, Google logs the IP addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crimes under investigation. Such information allows investigators to understand the geographic and chronological context of account access, use, and events relating to the crime under investigation.

9. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the user's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

10. Other information connected to an account may lead to the discovery of additional evidence. For example, the identification of other internet services and applications used may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

11. Therefore, the Providers' servers are likely to contain stored electronic communications and information concerning subscribers and their use of the Providers' services.

In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

D. Jurisdiction and Authority to Issue Warrants

12. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Providers, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

13. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

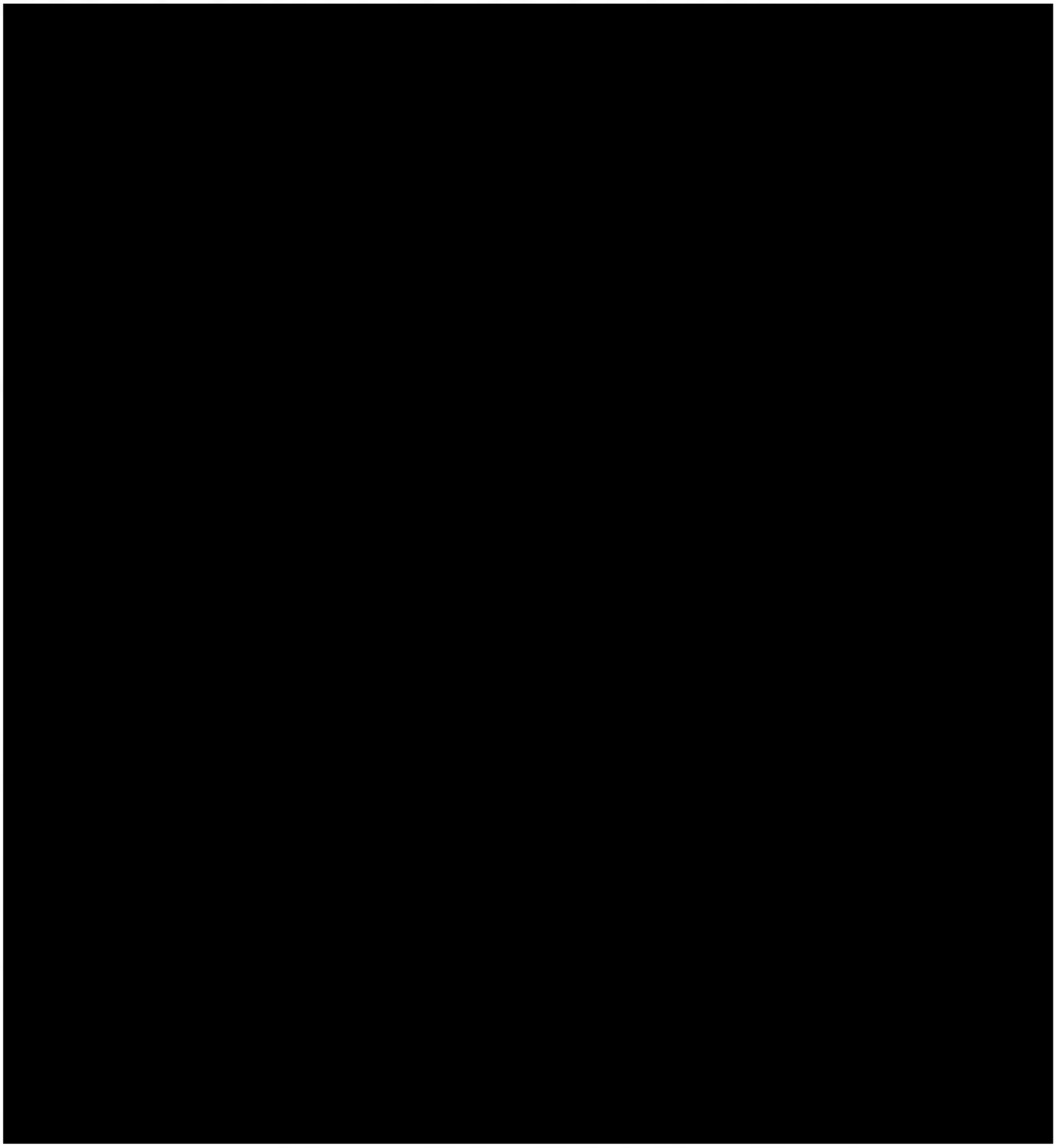
14. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Providers from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

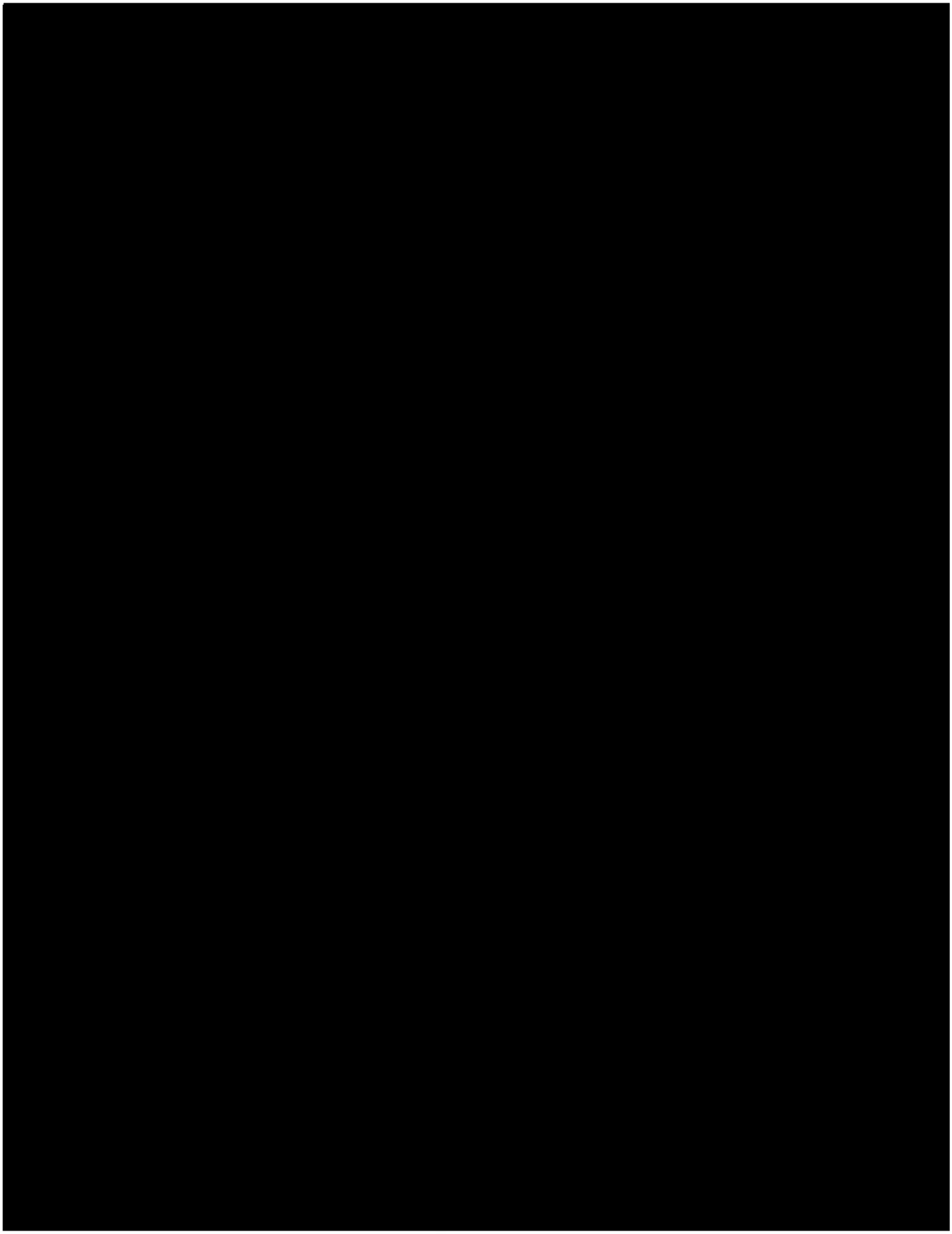
II. Probable Cause

A. Probable Cause Regarding the Subject Offenses

15. As set forth below, the Subject Offenses relate to a suspected scheme by several individuals to provide things of value to the then-romantic partner (and now wife) of U.S. Senator Robert Menendez in exchange for Menendez's influence attempting to secure a favorable

resolution of a New Jersey state criminal prosecution then pending against one of the individuals, and potentially in exchange for Menendez taking other official acts as well.





[redacted]

19. Based on my participation in this investigation, including my conversations with other law enforcement officers who debriefed the CS, and my review of a summary translation of a recording made by the CS and law enforcement reports concerning the same, I have learned that in or about August 2019, *i.e.*, shortly after the plea and sentencing described above,[5] the CS met with [redacted] and the following occurred, in substance and in part:

[redacted]

[5] Based on my review of law enforcement reports, I believe that [redacted] and Hana had a financial dispute, possibly prior to this conversation.

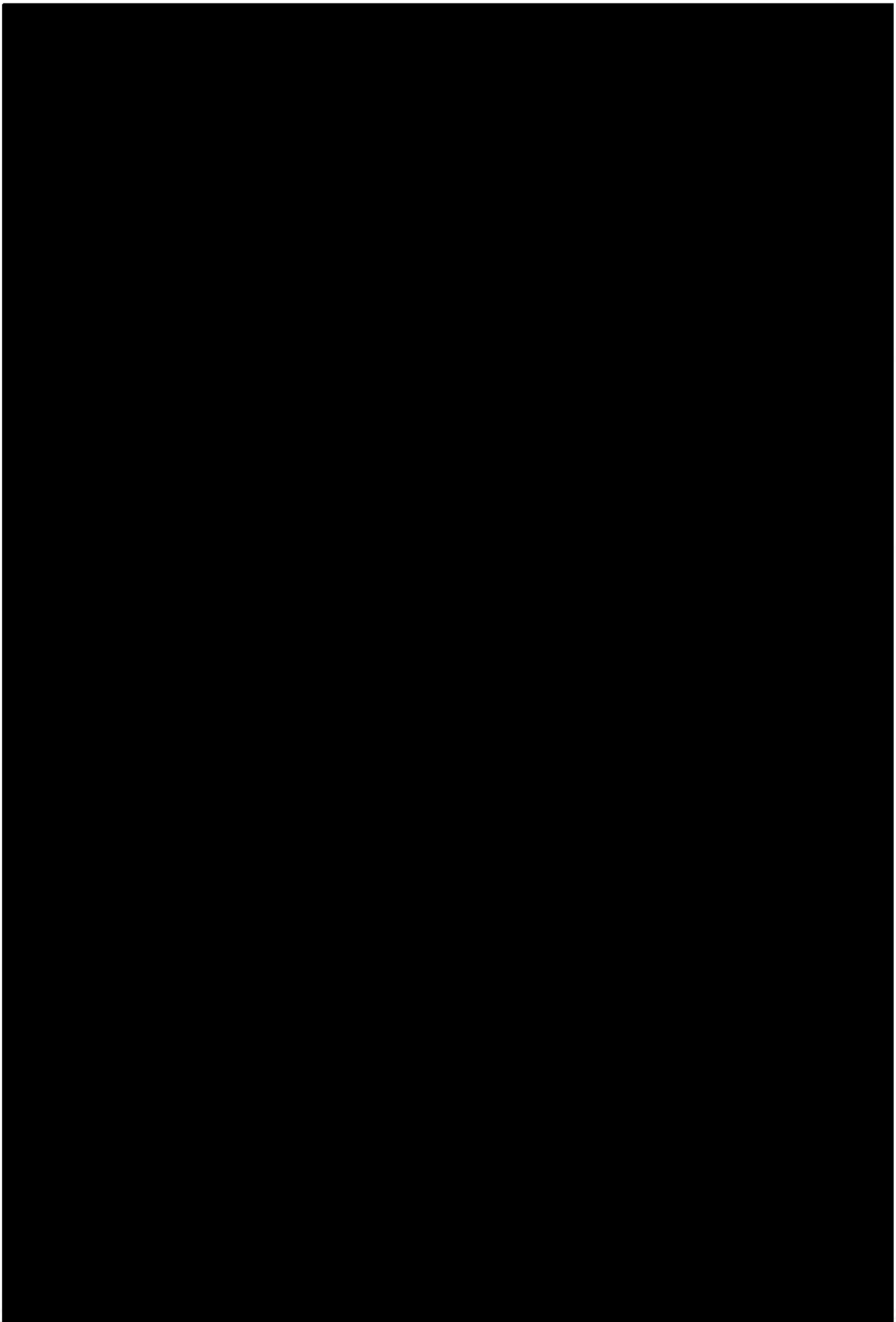
a. [redacted] told the CS, in sum and substance, that Hana arranged for Arslanian to receive a ring and a car in exchange for Menendez's assistance in resolving criminal charges for insurance fraud pending against an American male.[6]

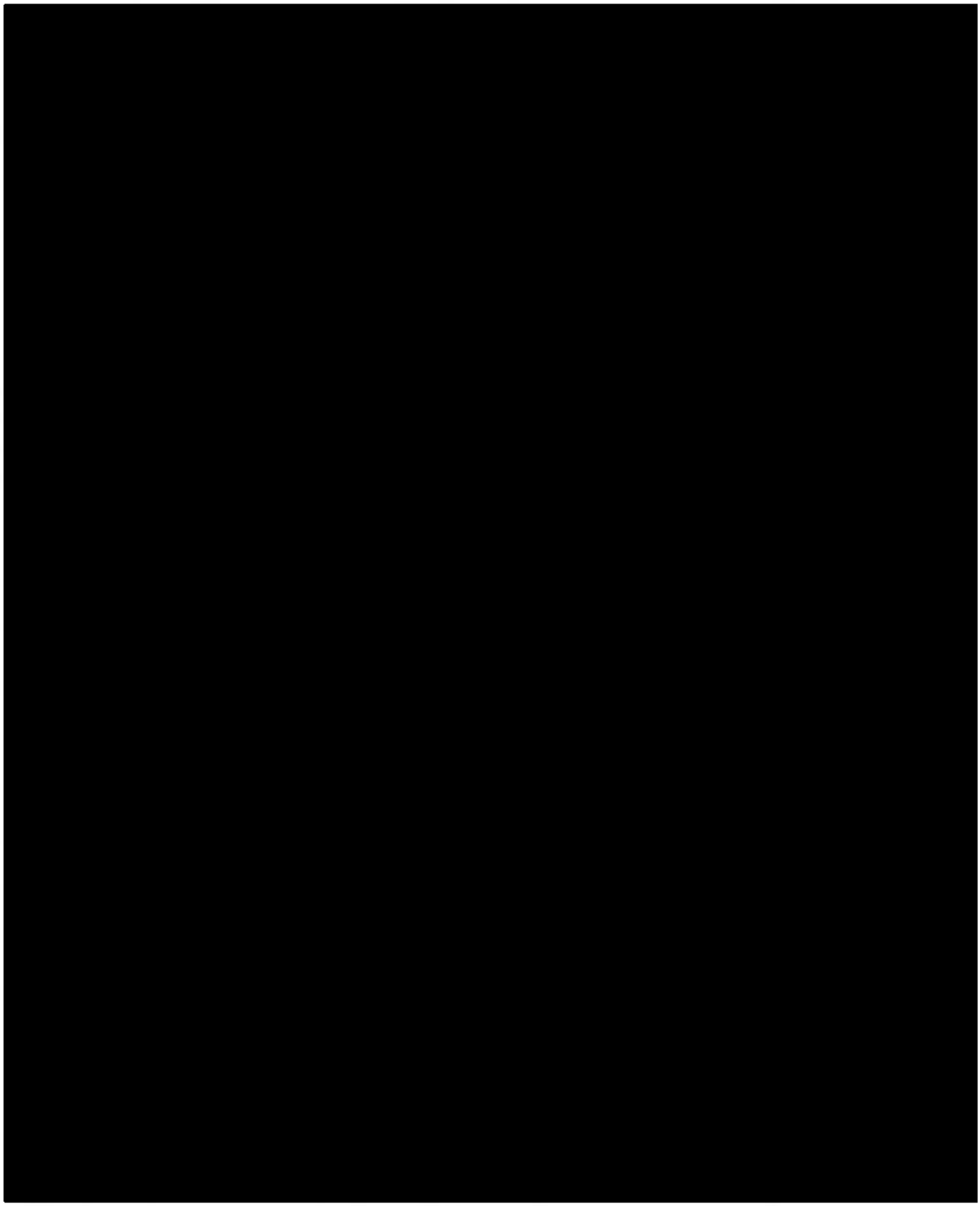
b. In particular, on the recording of this meeting made by the CS, [redacted] discussed how the criminal case "needed a push," and "this push saved the male three years."

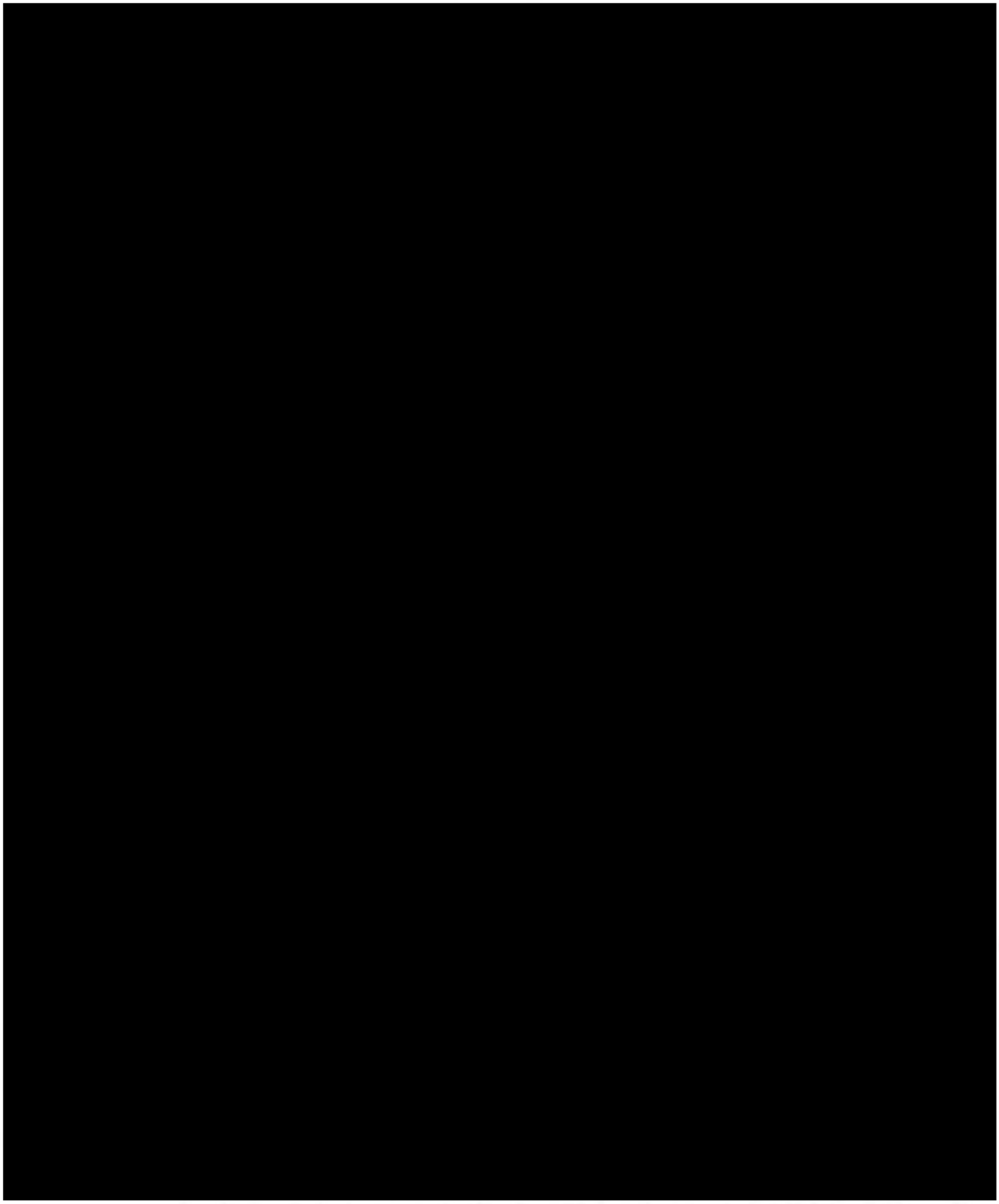
c. [redacted] further told the CS that the American male gave Hana $150,000 and that Hana then purchased the engagement ring for Menendez's girlfriend, along with a car, and kept the remaining money for himself. As detailed further below, I believe that the "American male" is a reference to [redacted]

[redacted]

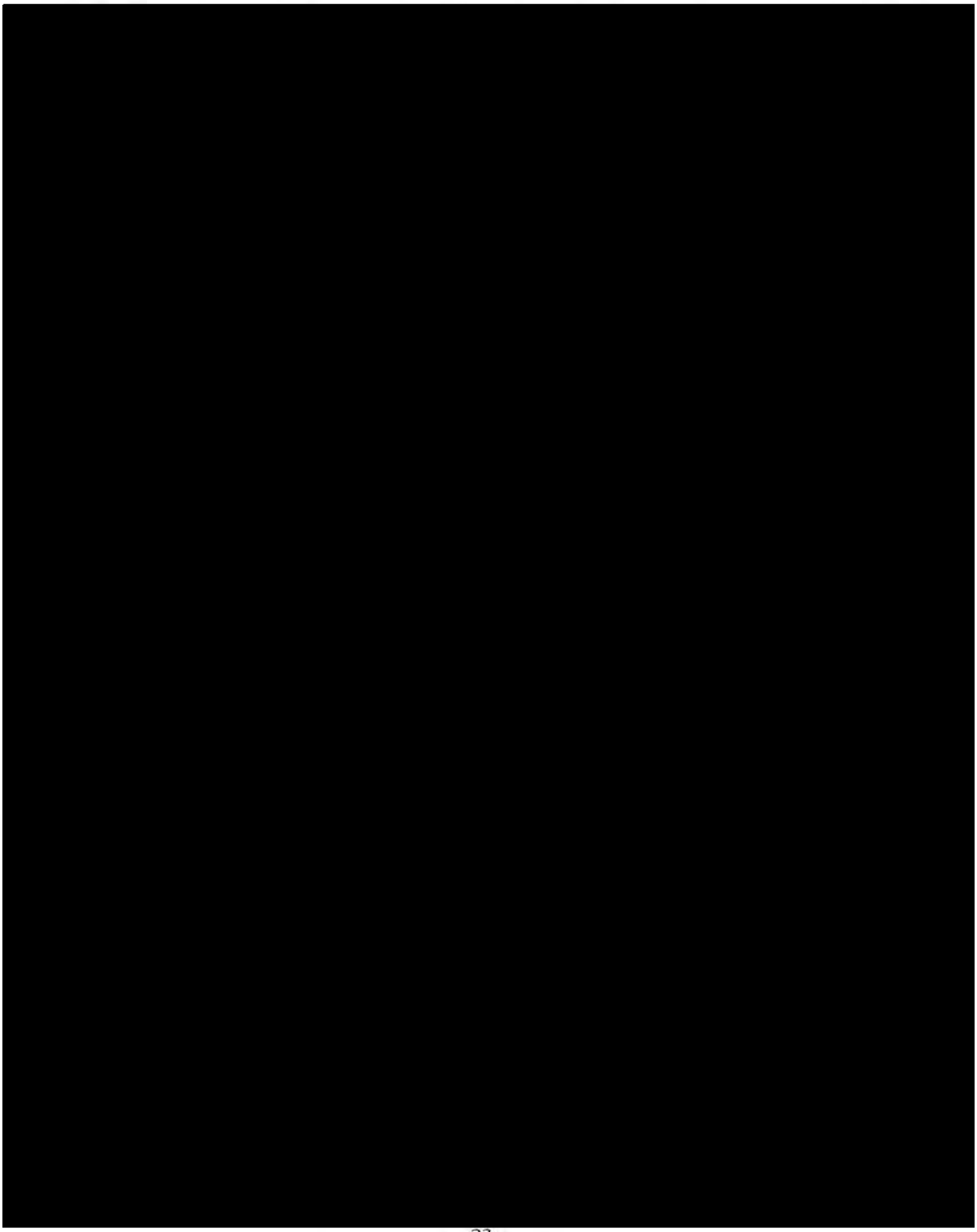
[6] These communications took place mainly in Arabic, and the description of them is based on a review of a draft summary and translation, subject to further revision.

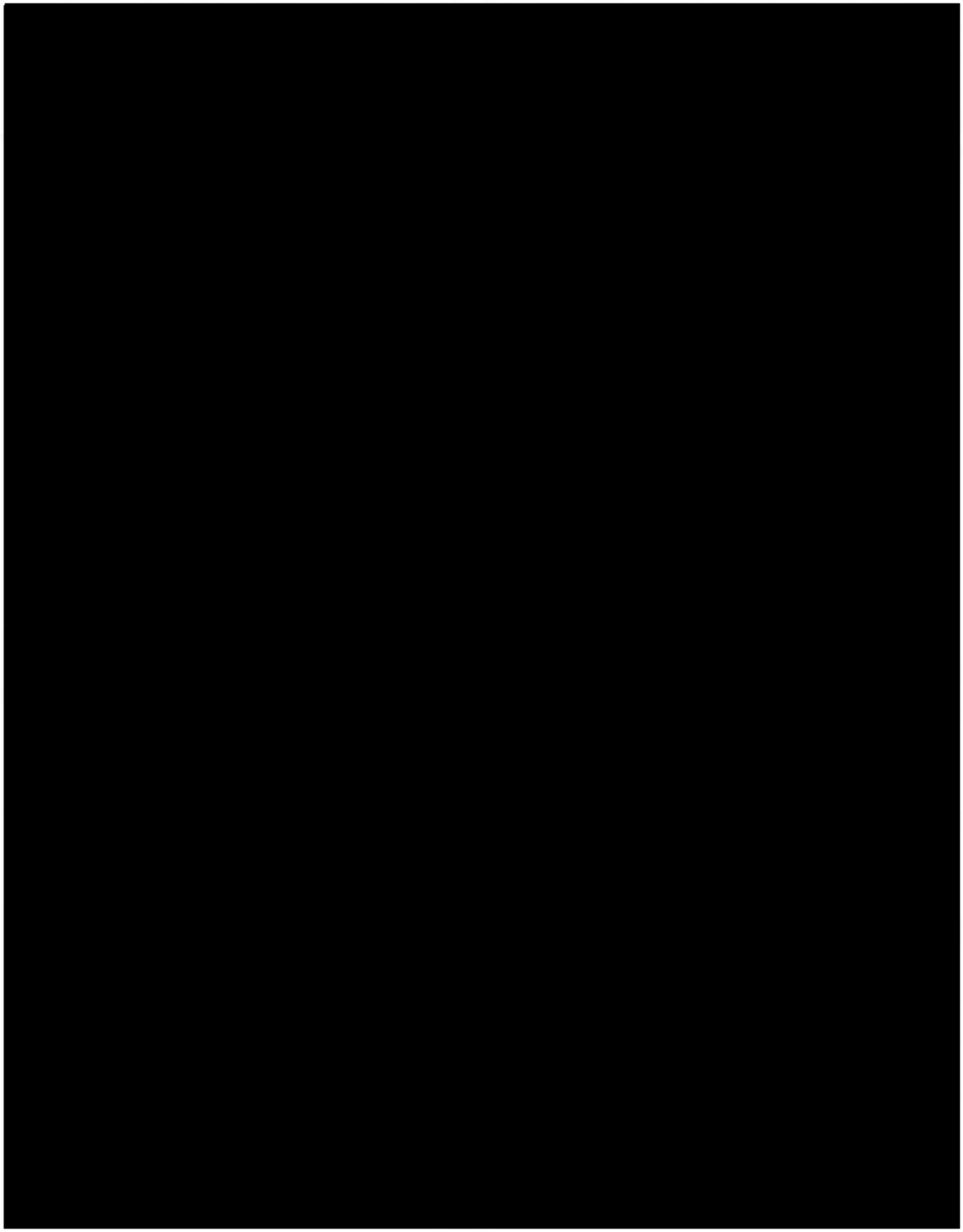


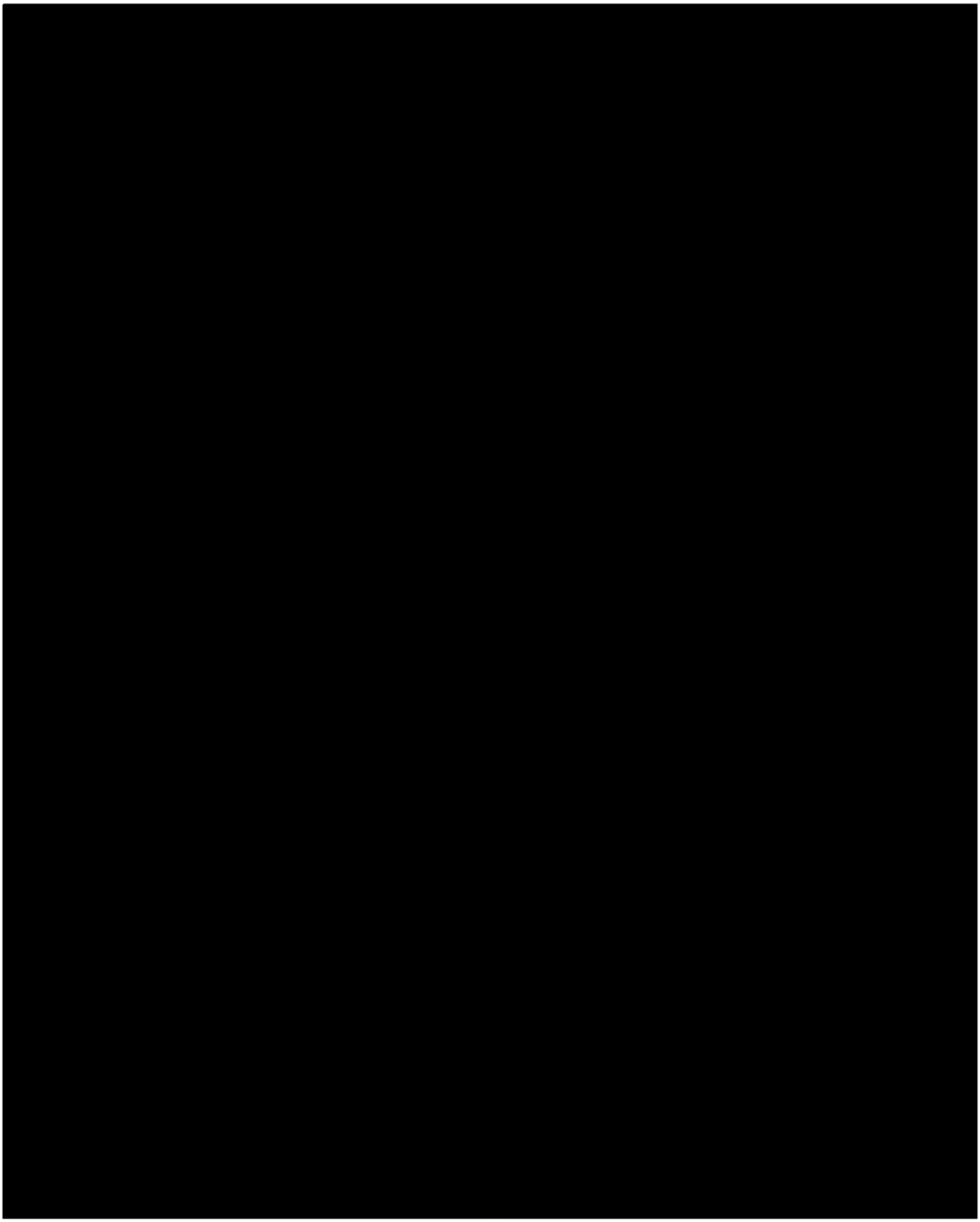


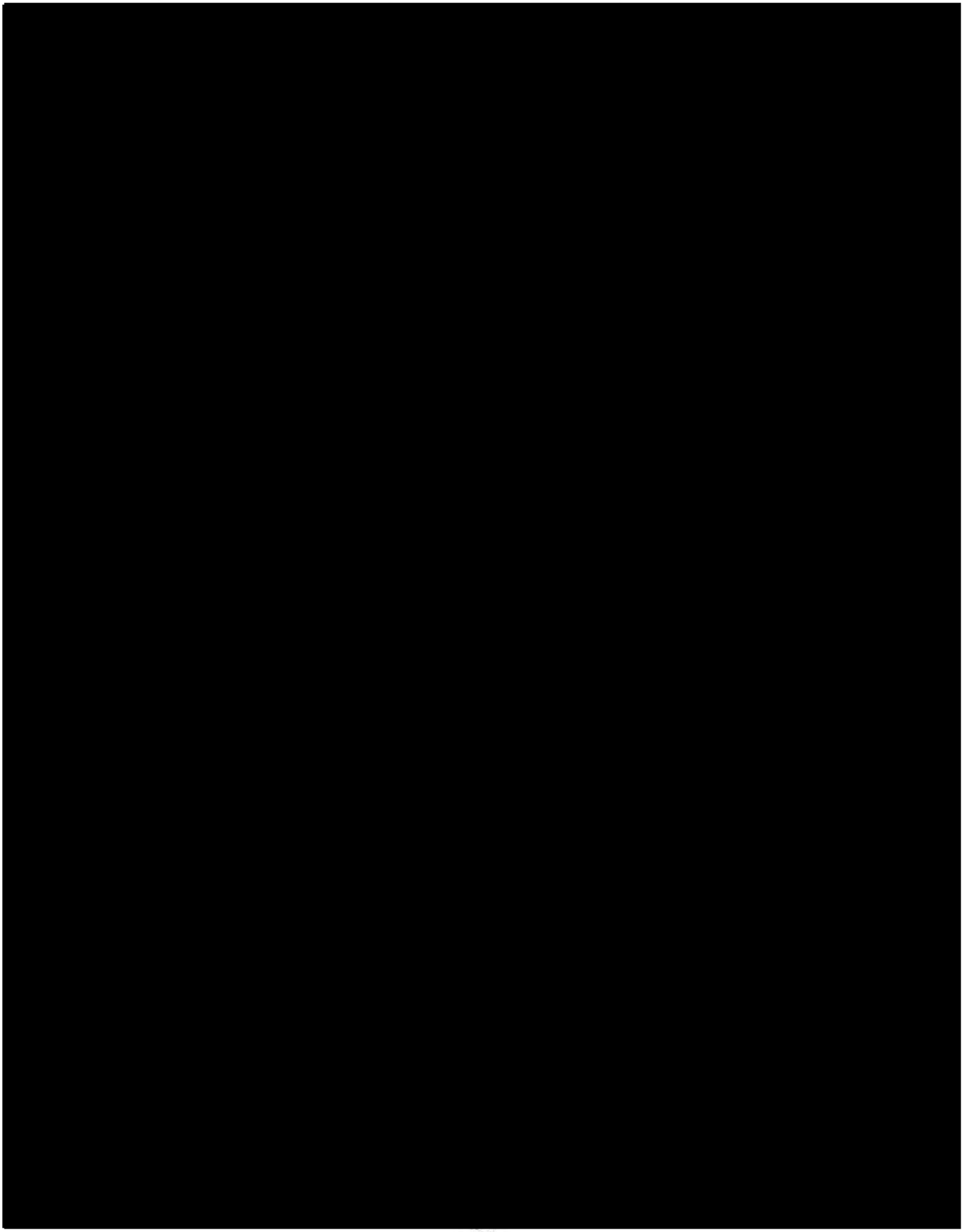


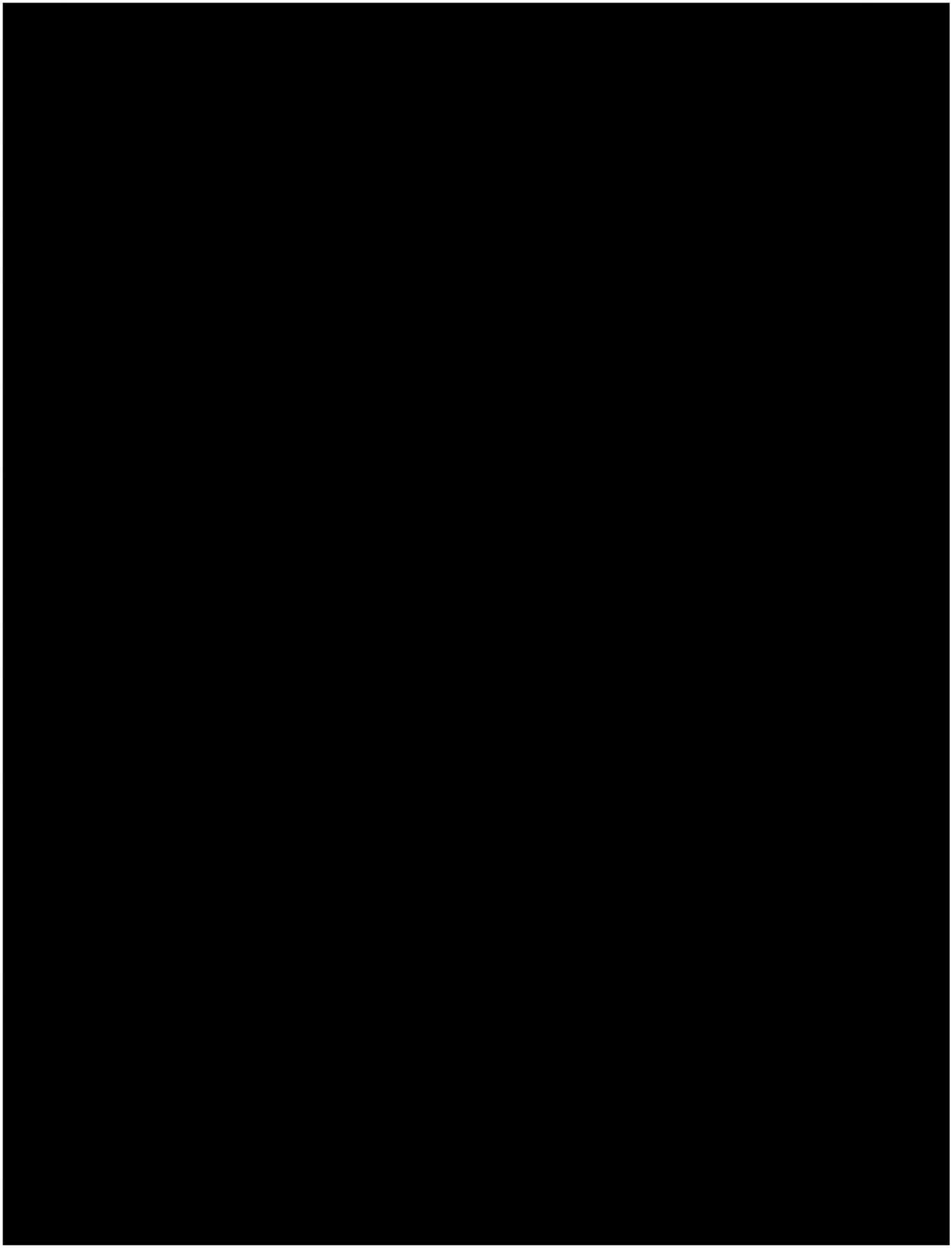
c. Later on April 4, 2018, Uribe messaged Hana, writing, "The deal is to kill and stop all investigation. [redacted]

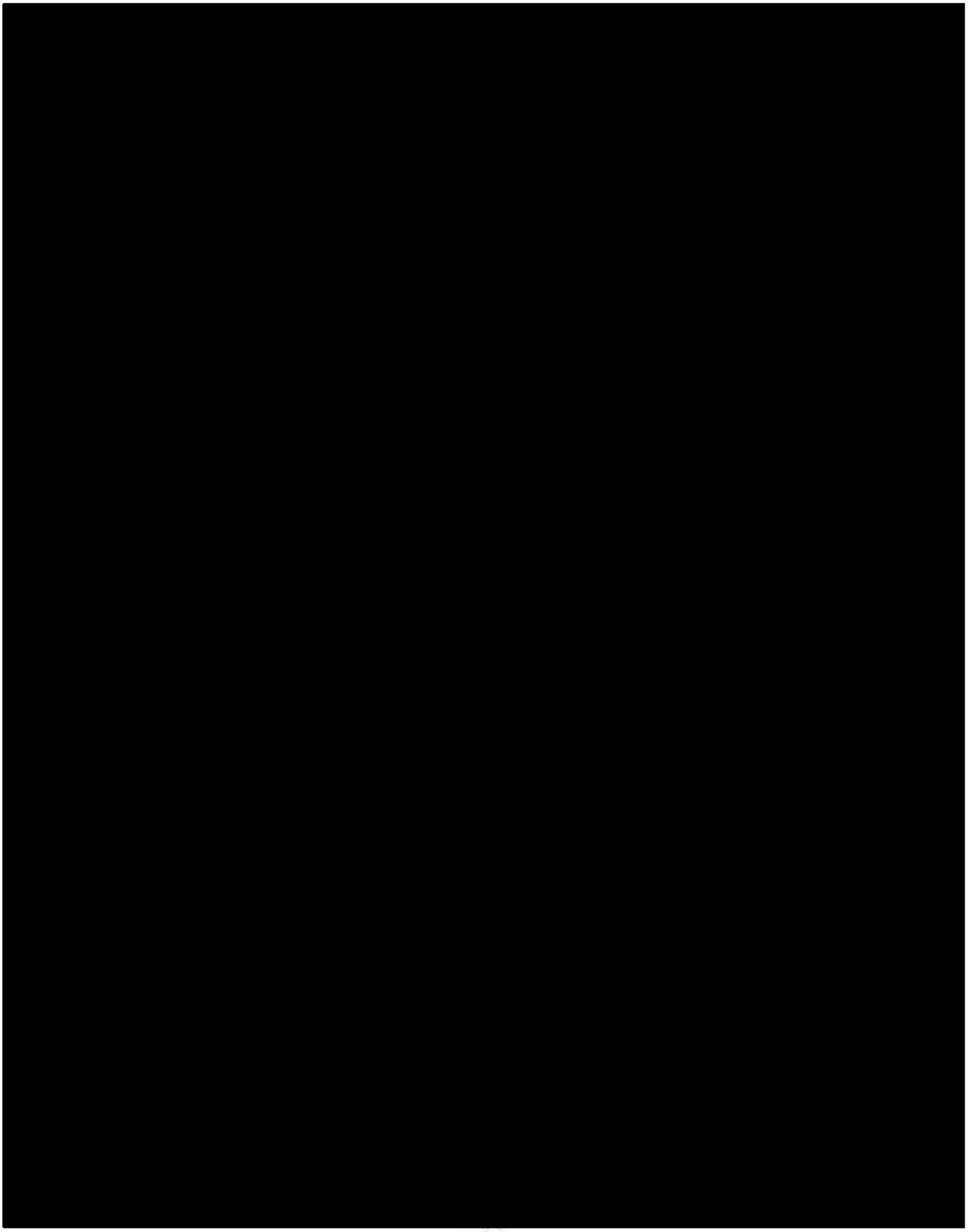


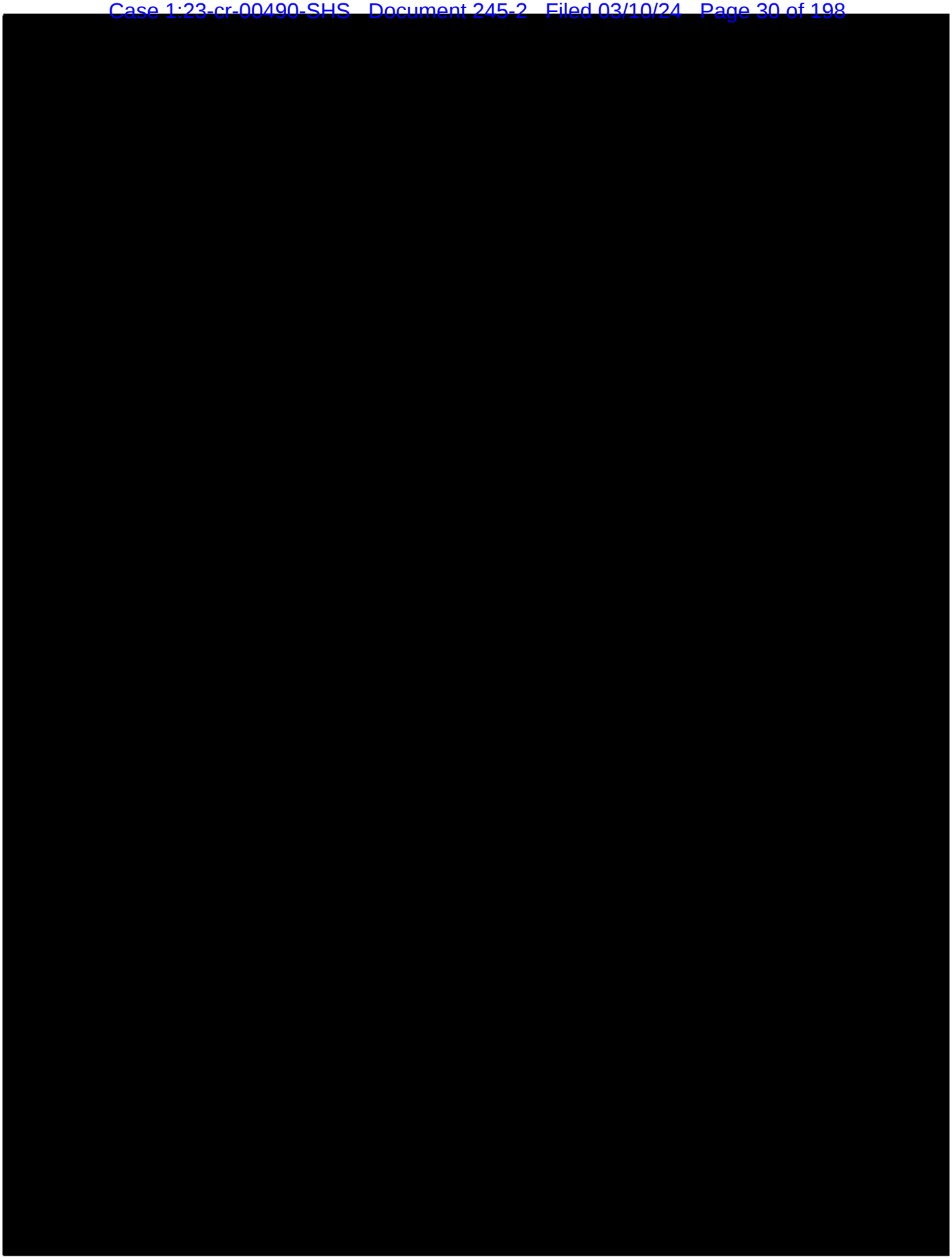


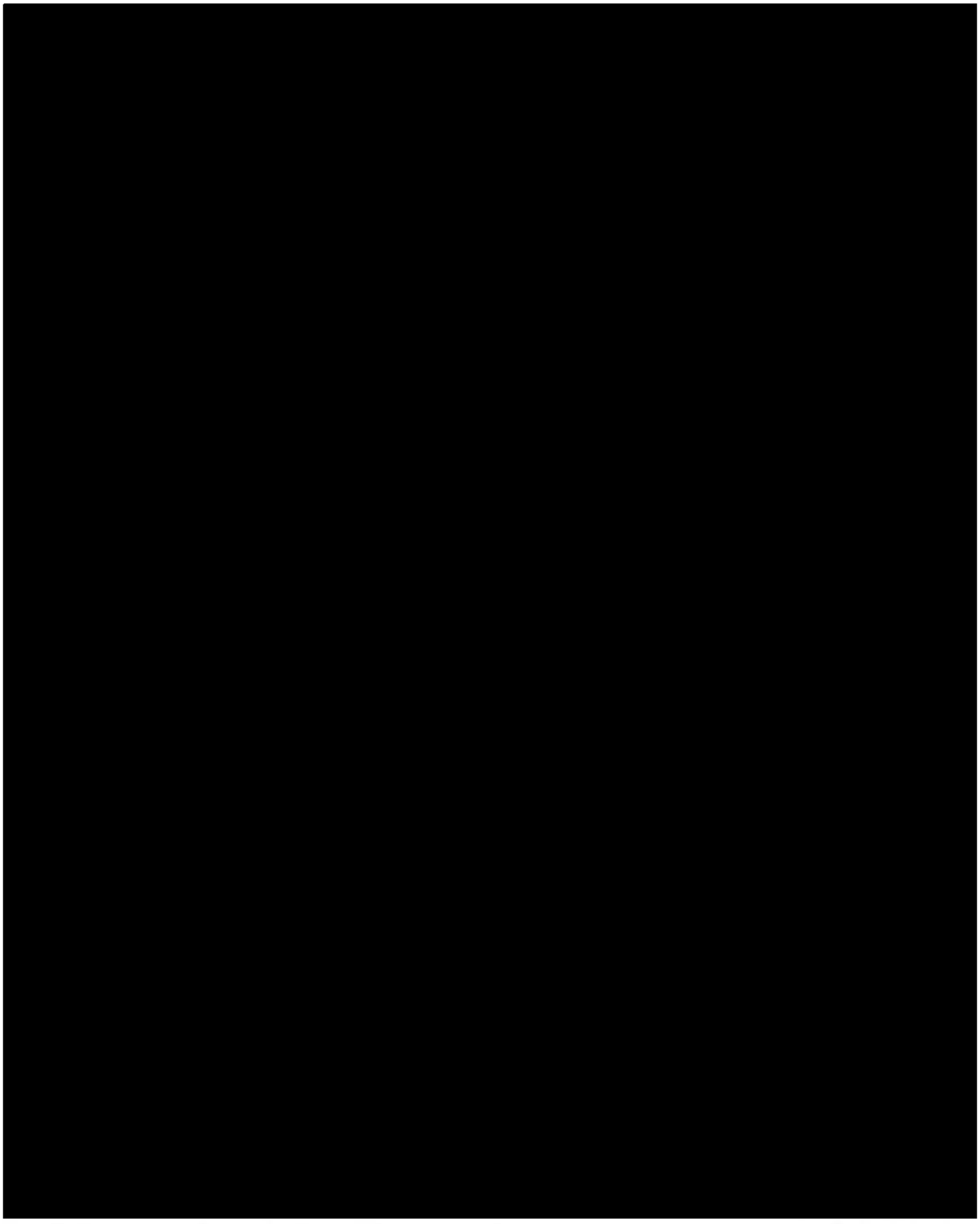


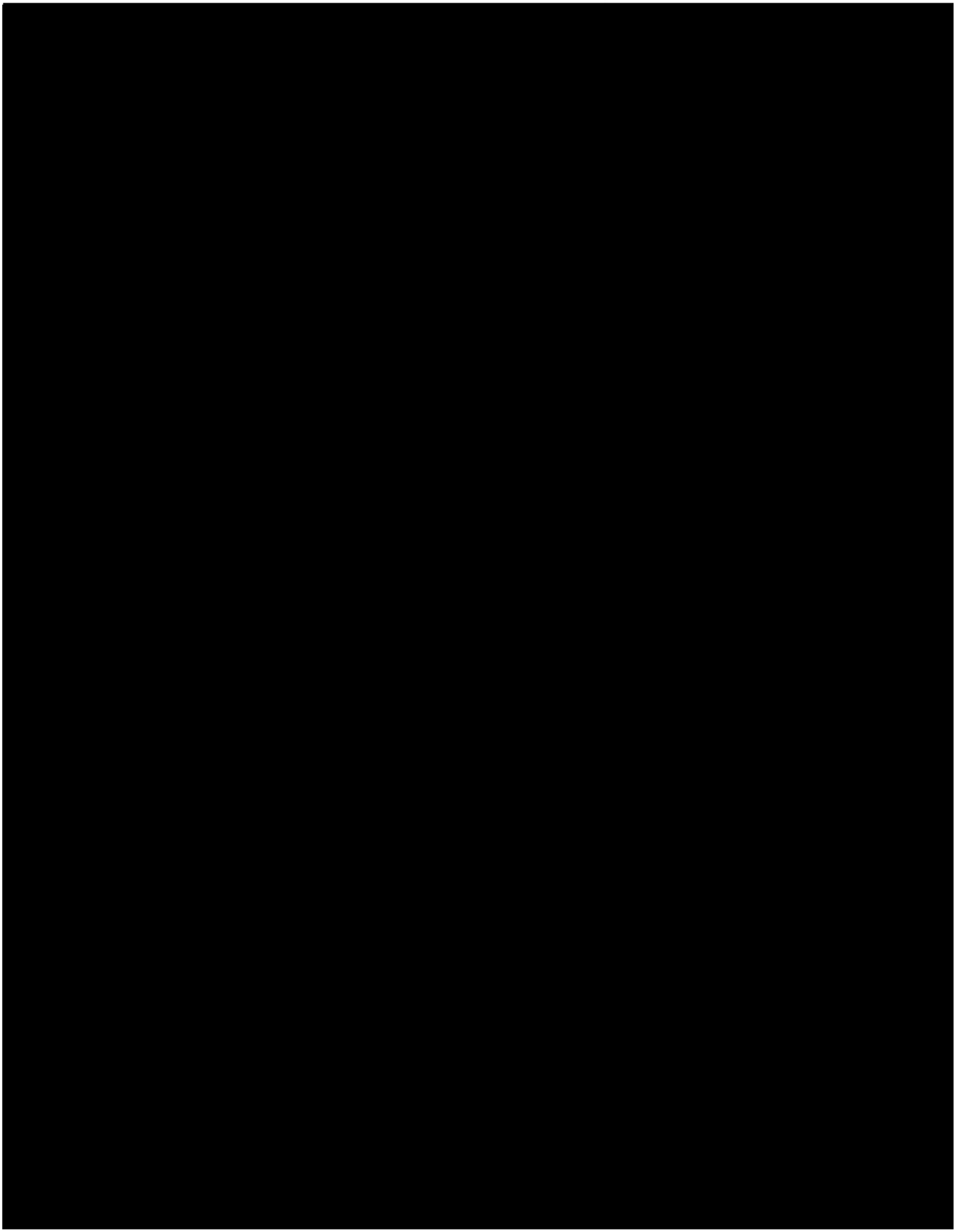


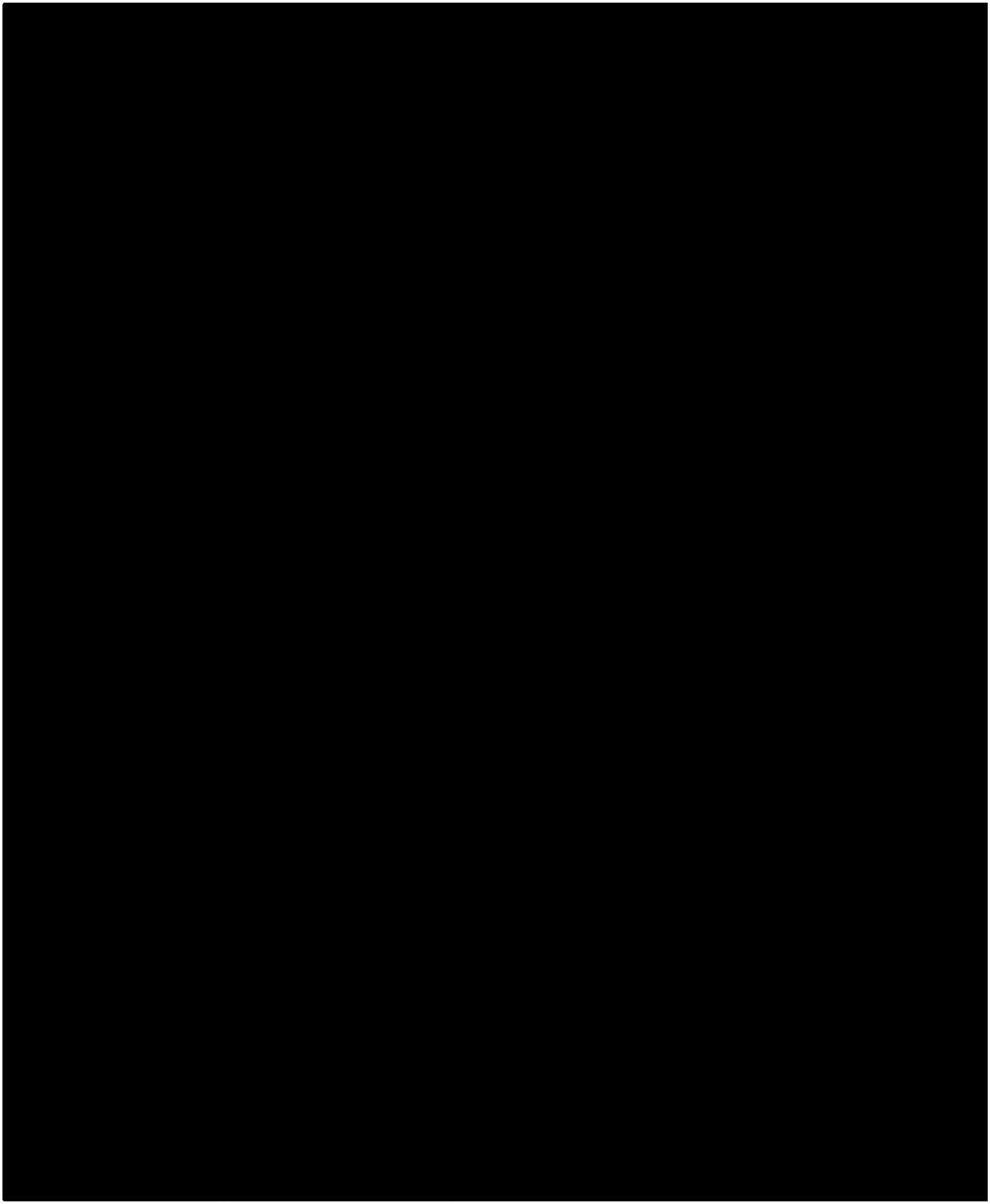


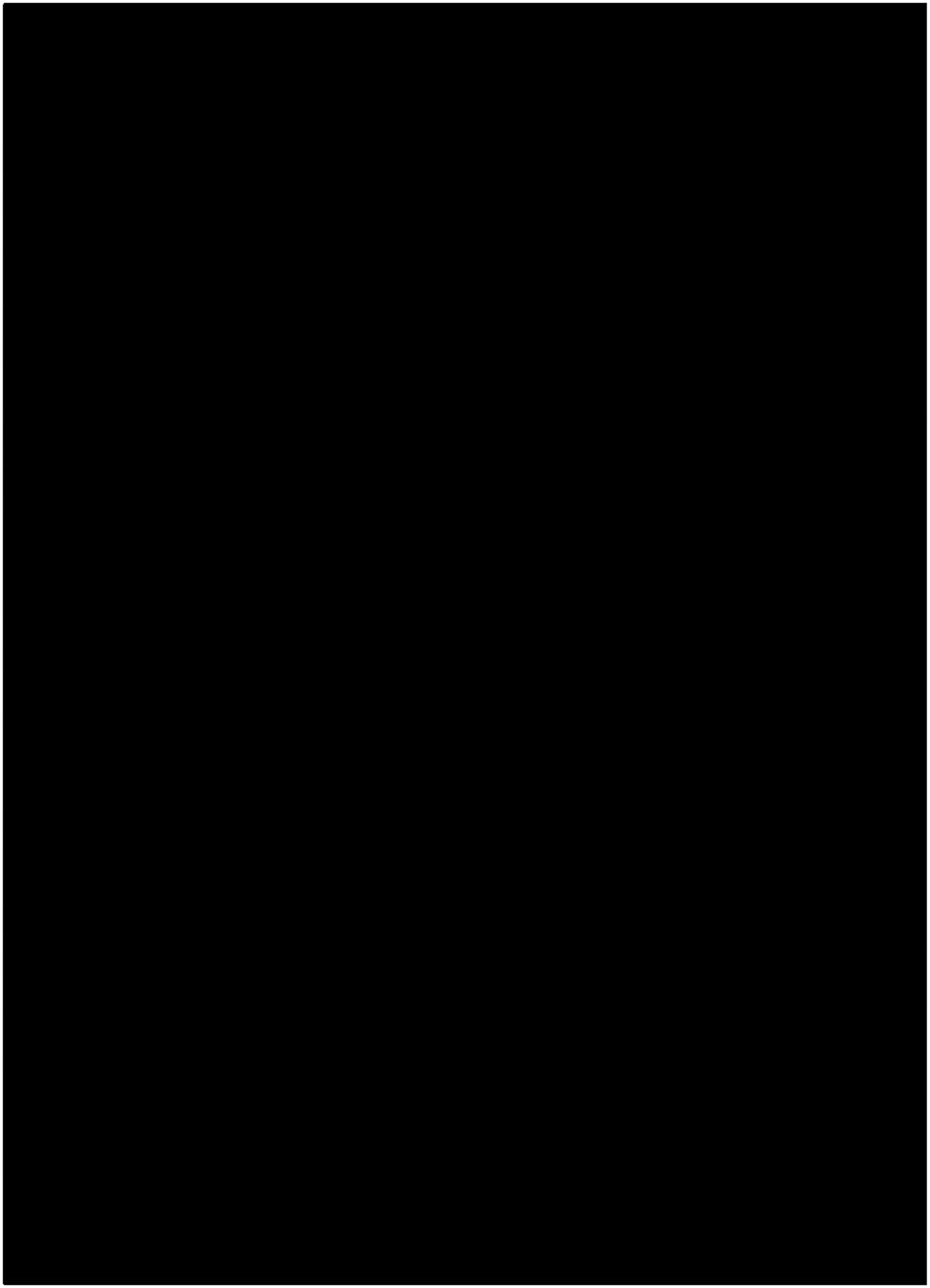


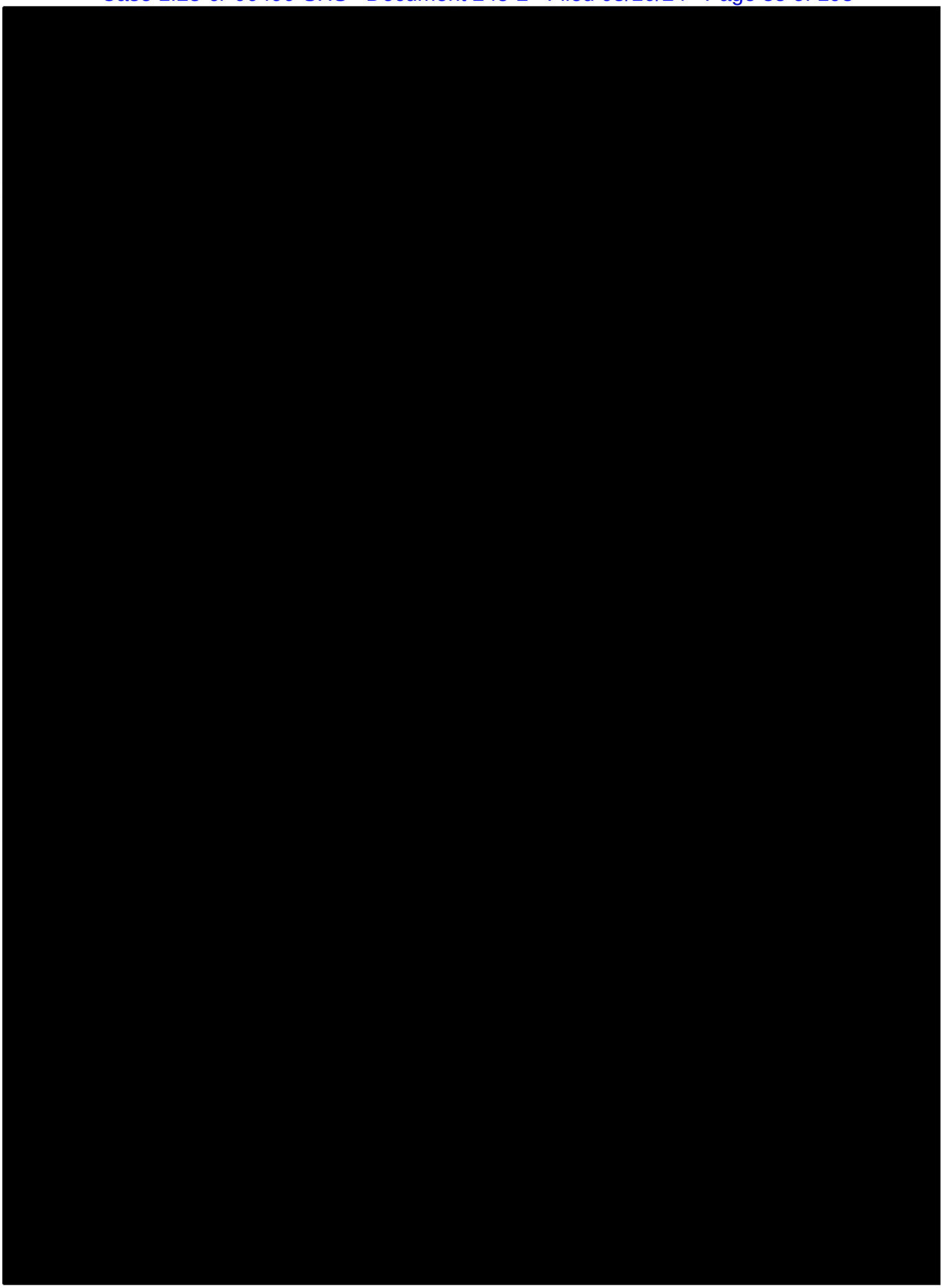


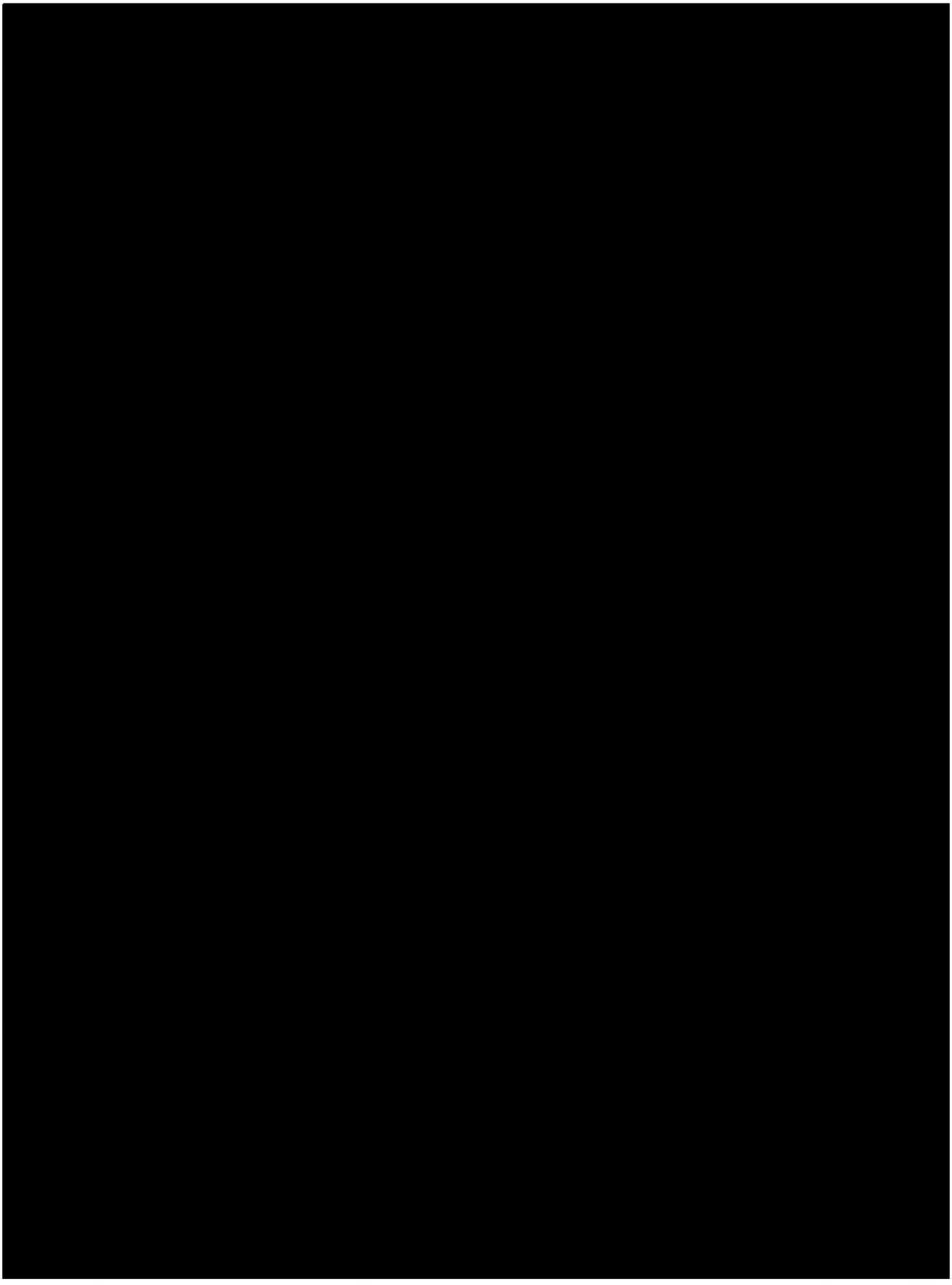


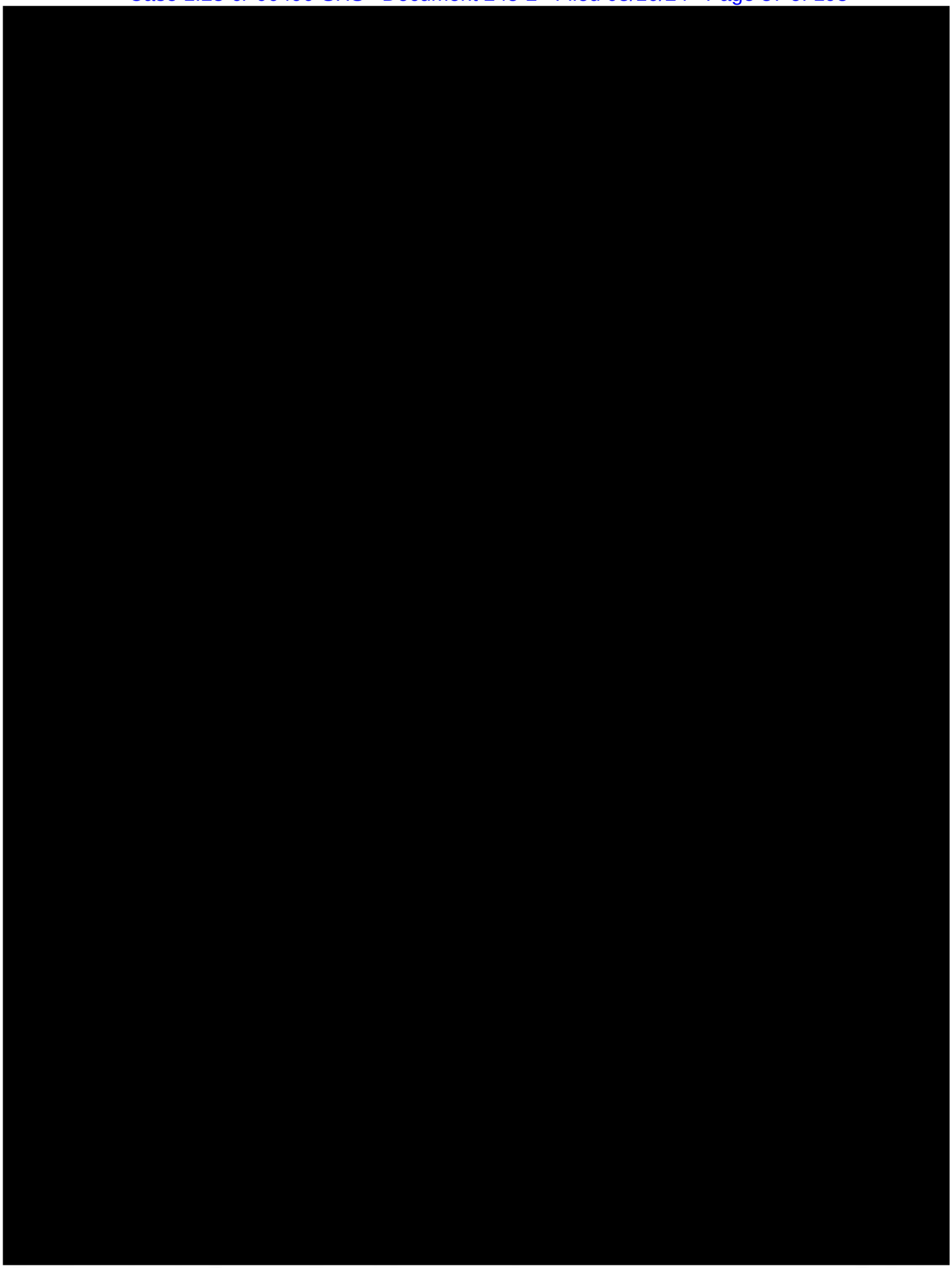


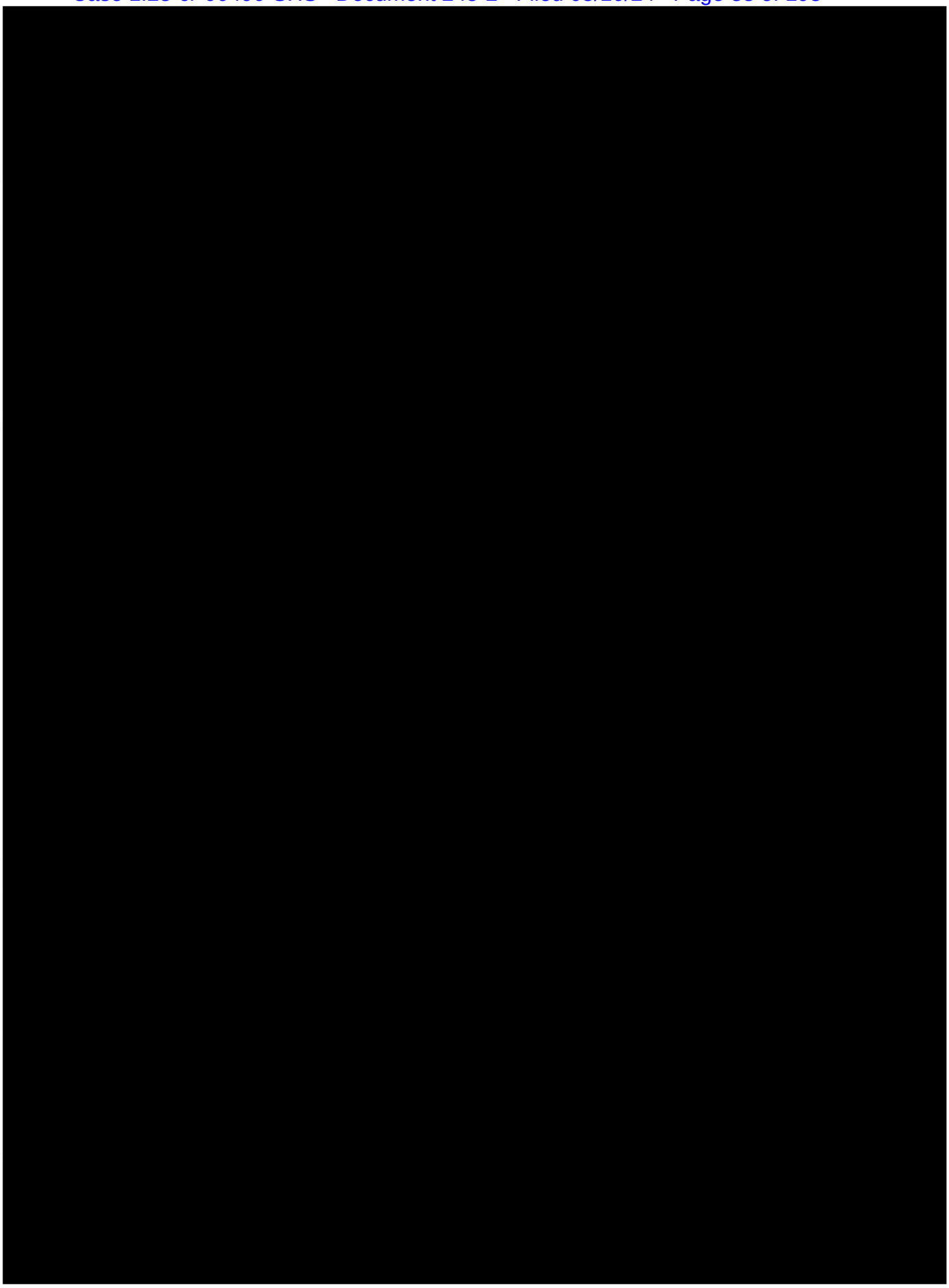


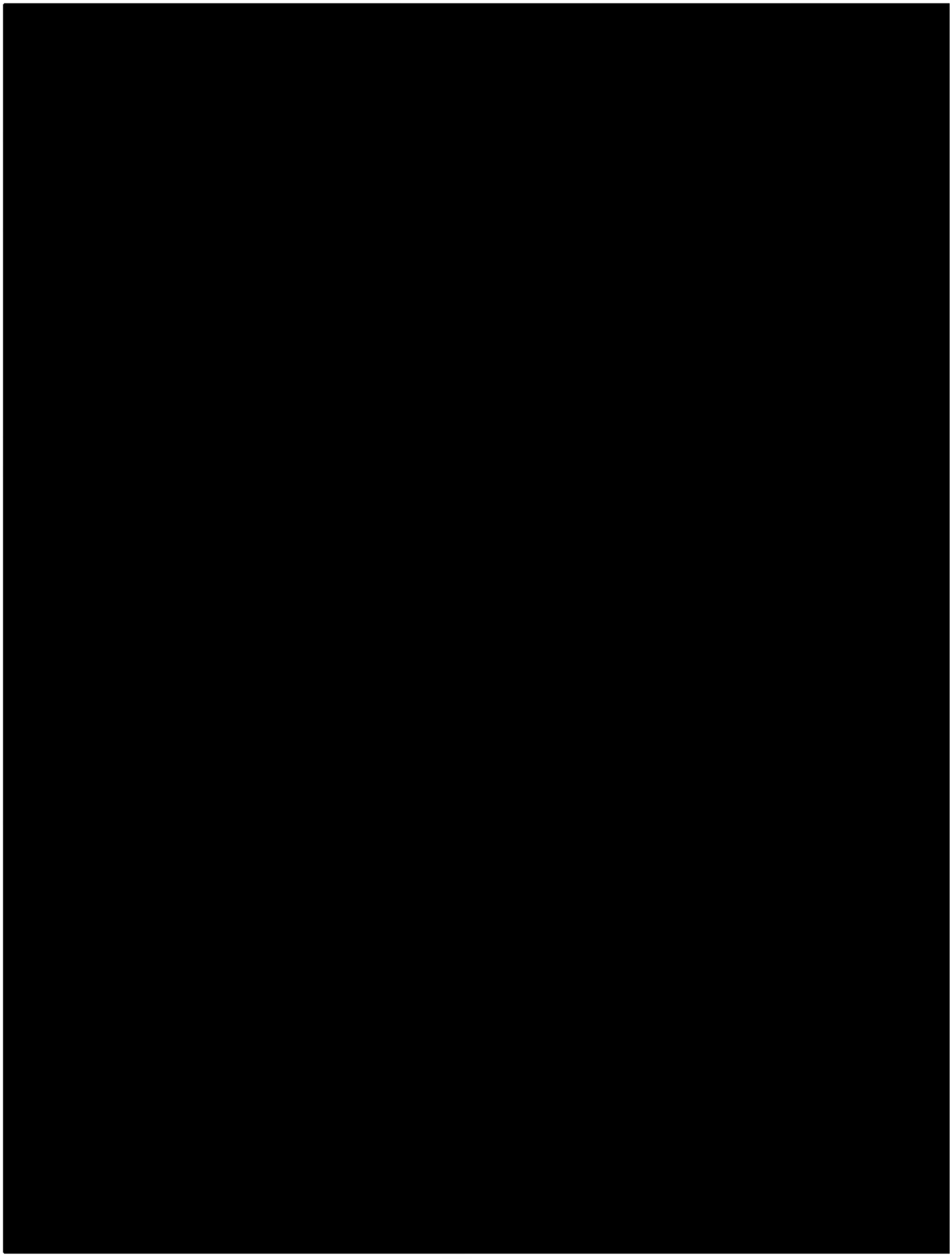


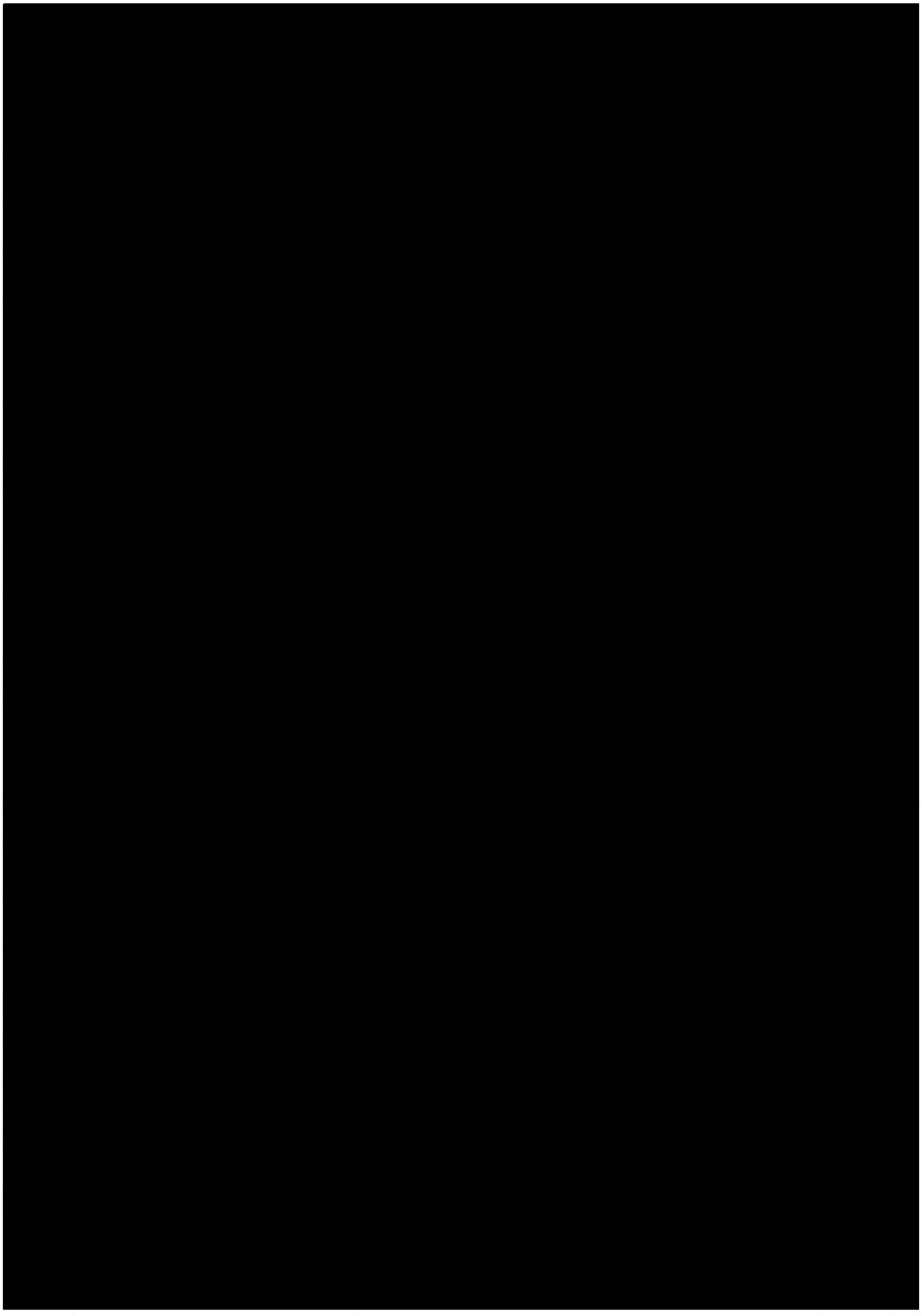


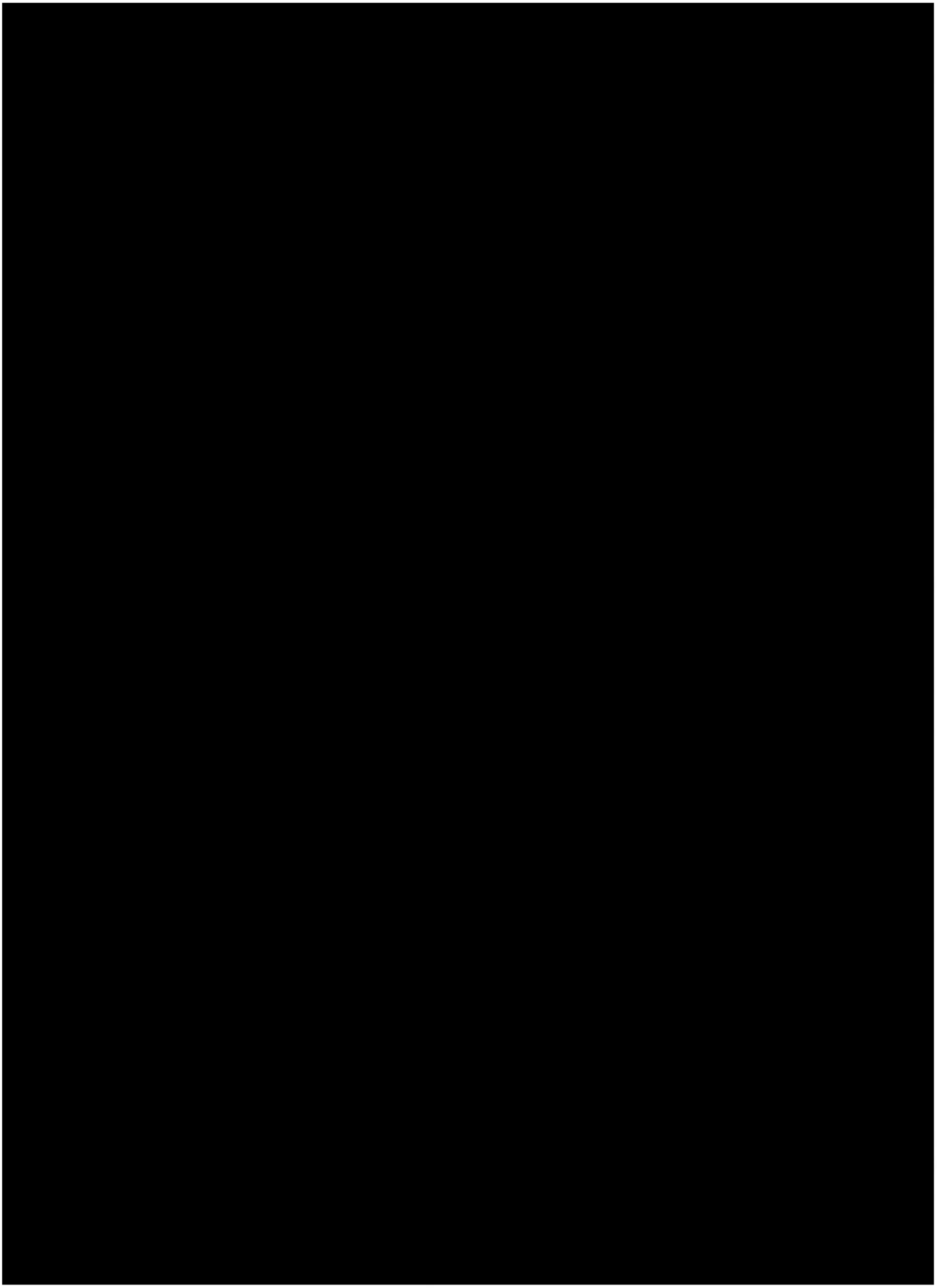








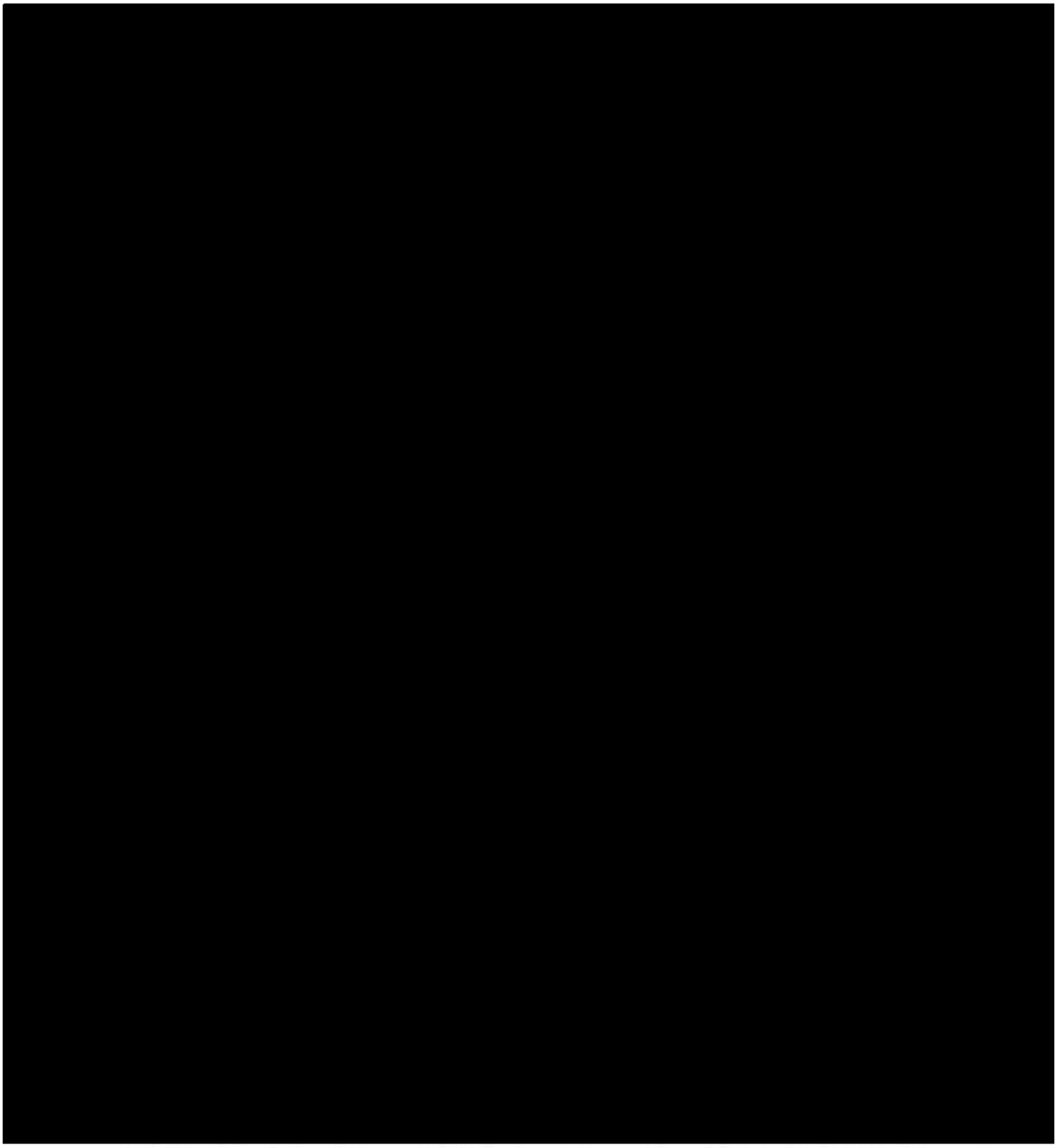




[redacted]

Additional Acts and Things of Value Requested and Exchanged

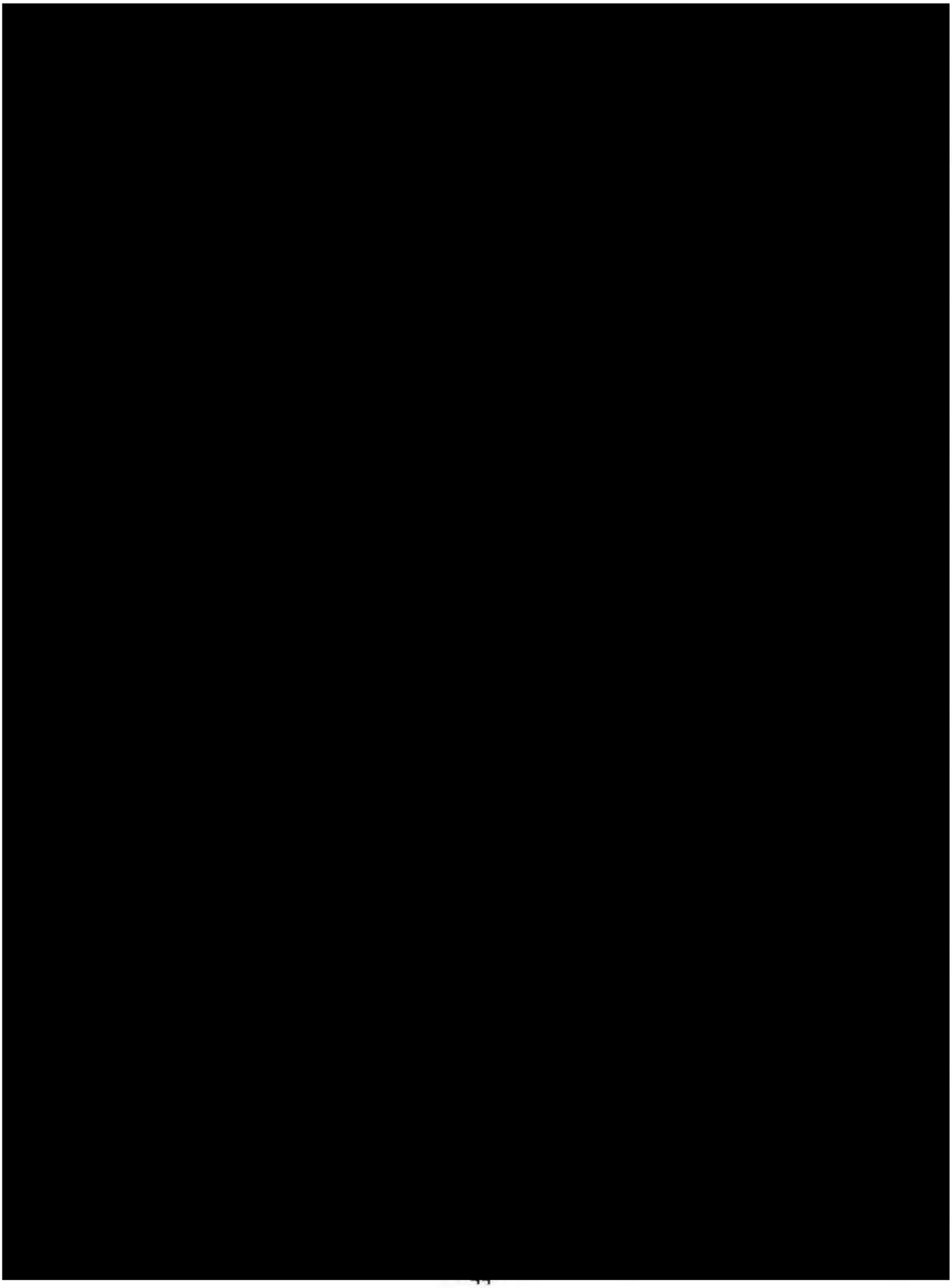
40. As set forth below, I believe that Uribe sought some sort of action from Menendez regarding a cancer fundraiser, and met with Menendez in April 2019. [redacted]

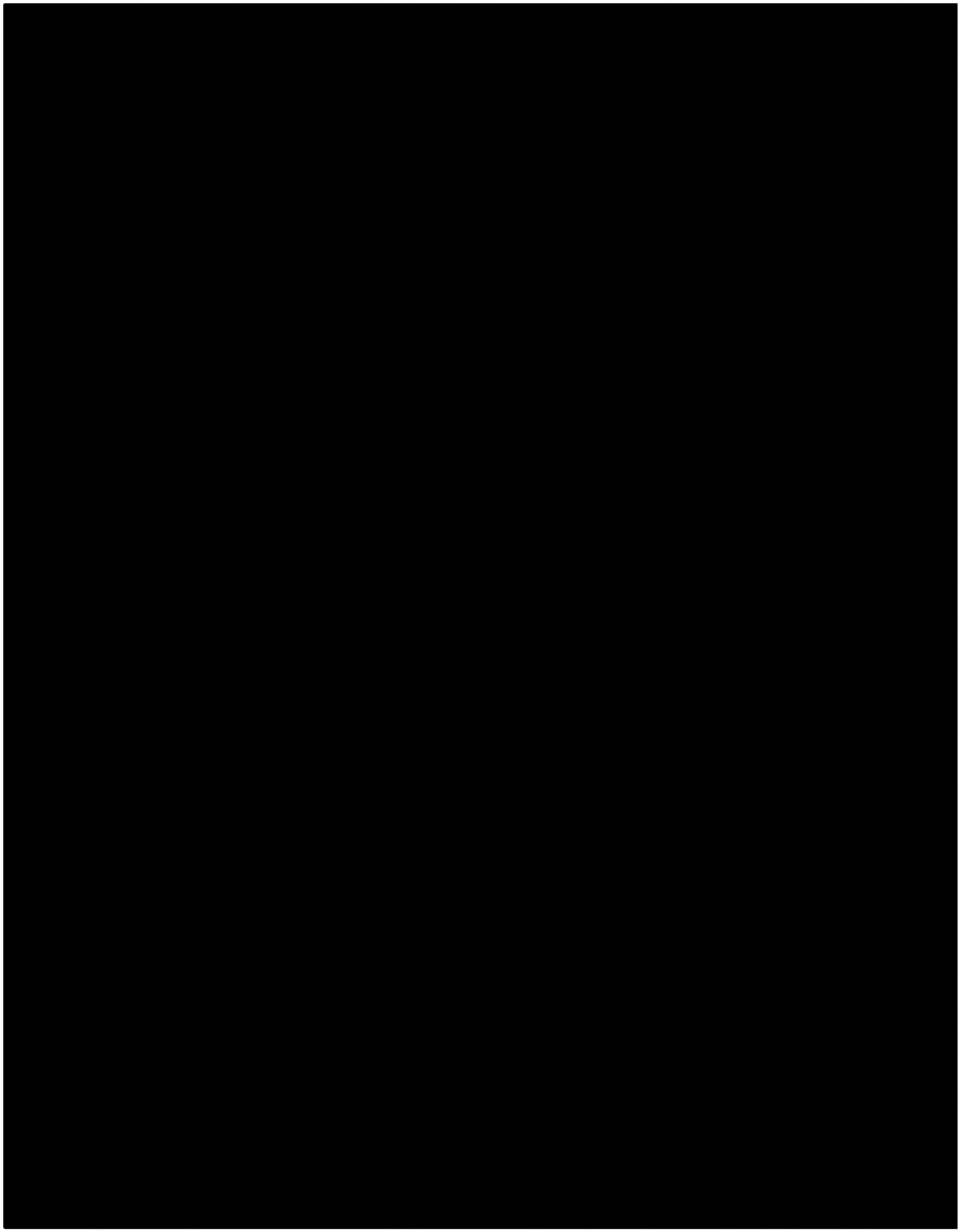


41. As set forth below, I believe that Hana sent Arslanian documents requesting assistance from Menendez with respect to two official proceedings—a United States Department of

Agriculture ("USDA") investigation of the Hana Halal Company, and a personal injury lawsuit by a plaintiff seeking to access Egyptian assets. S

[redacted]

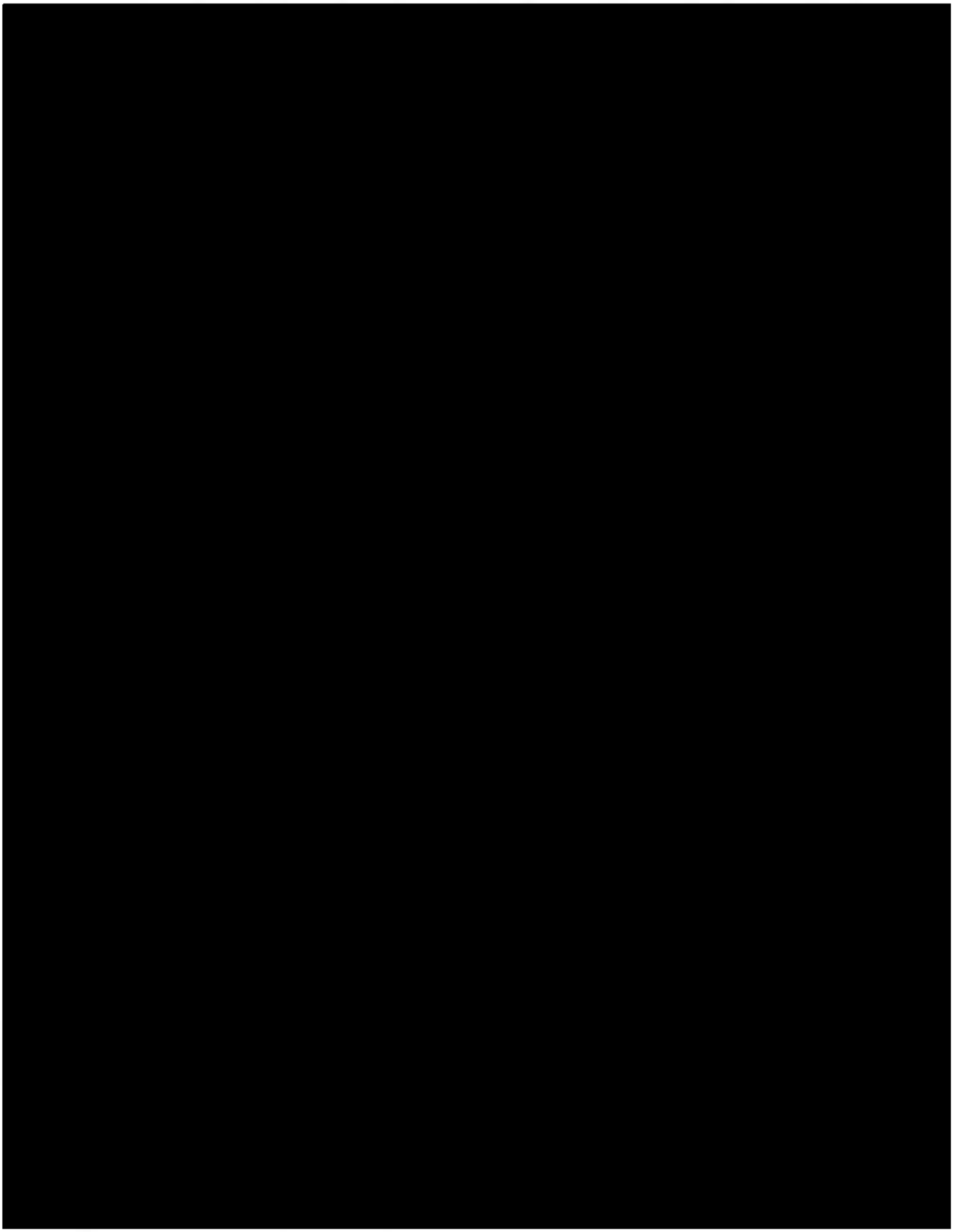


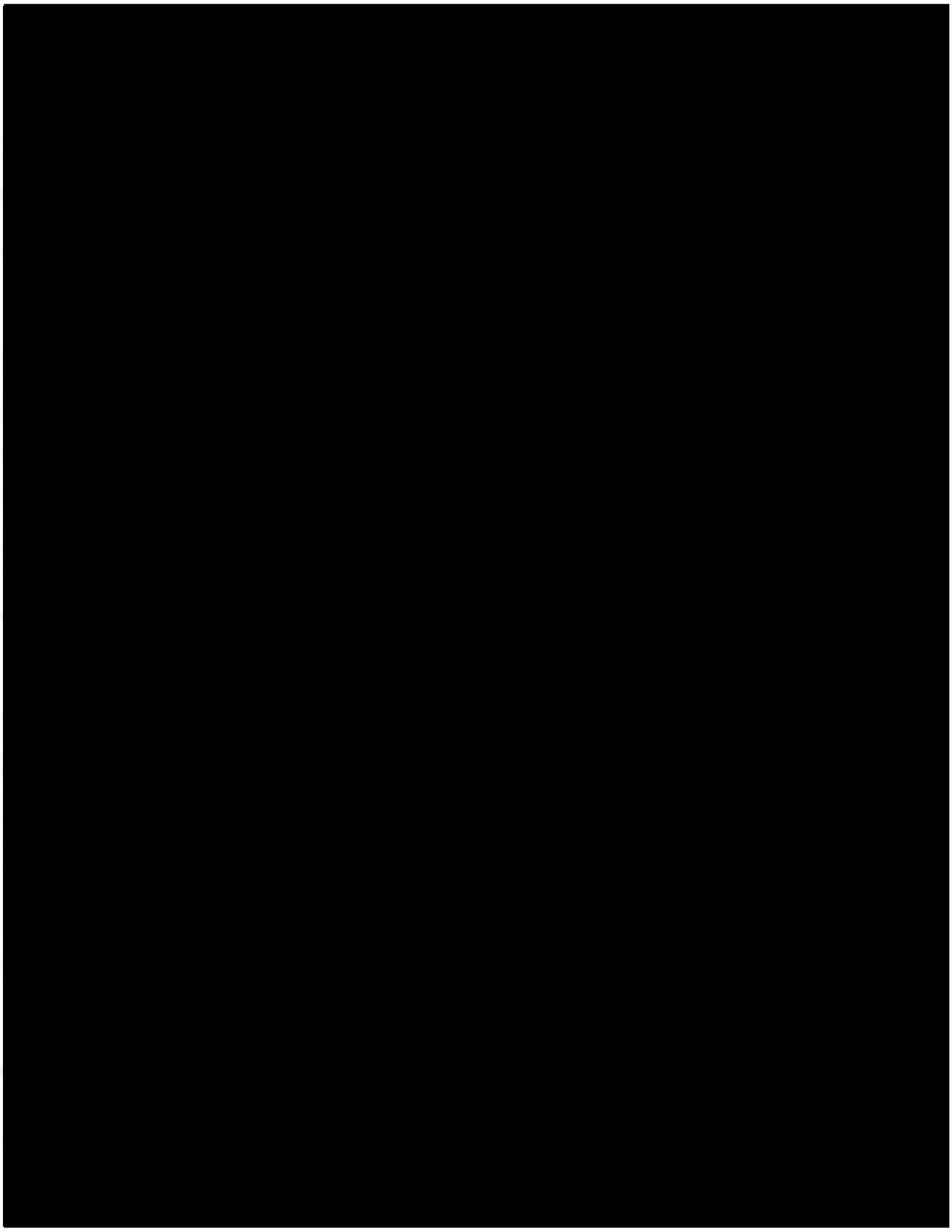


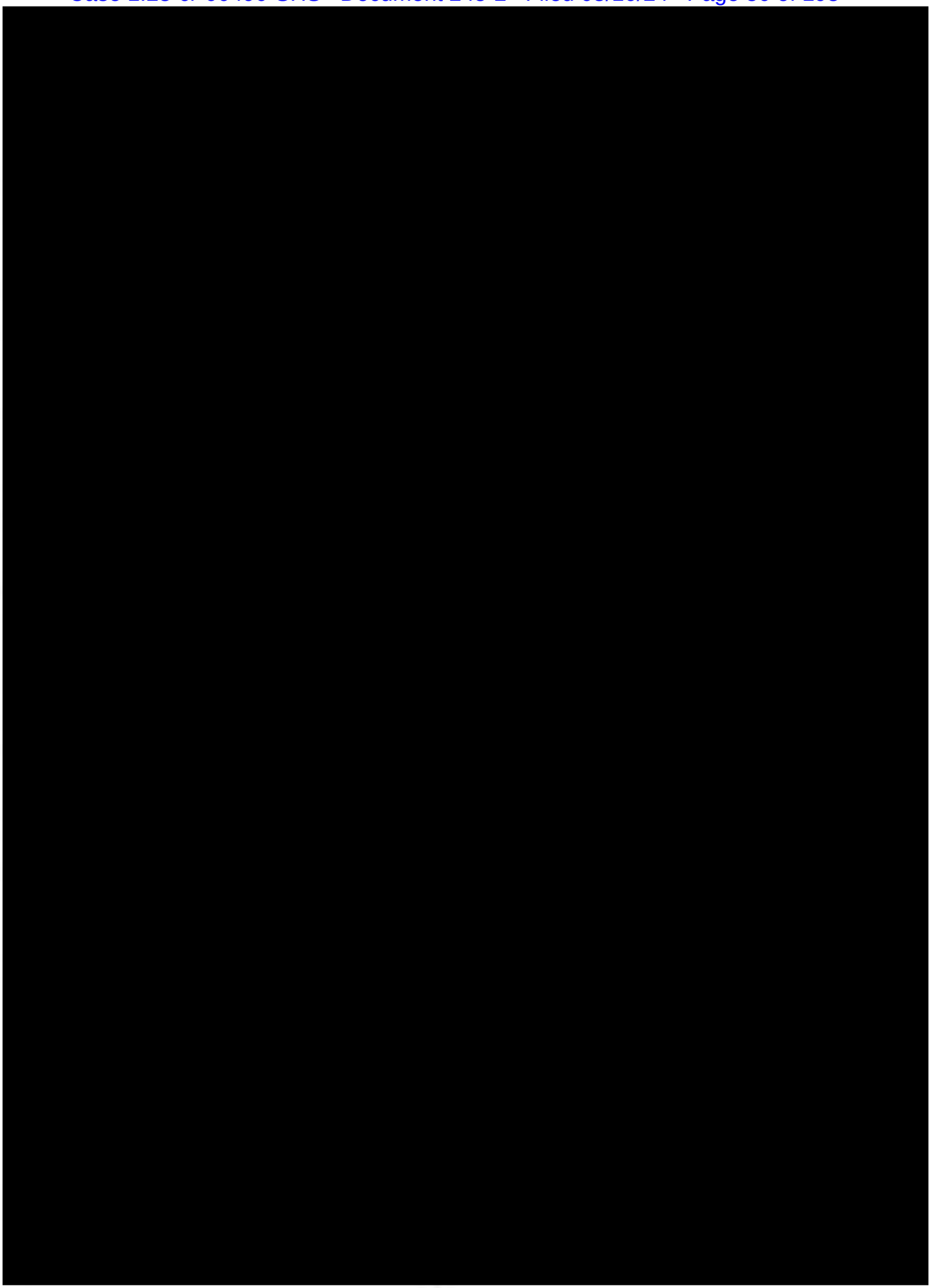
[redacted]

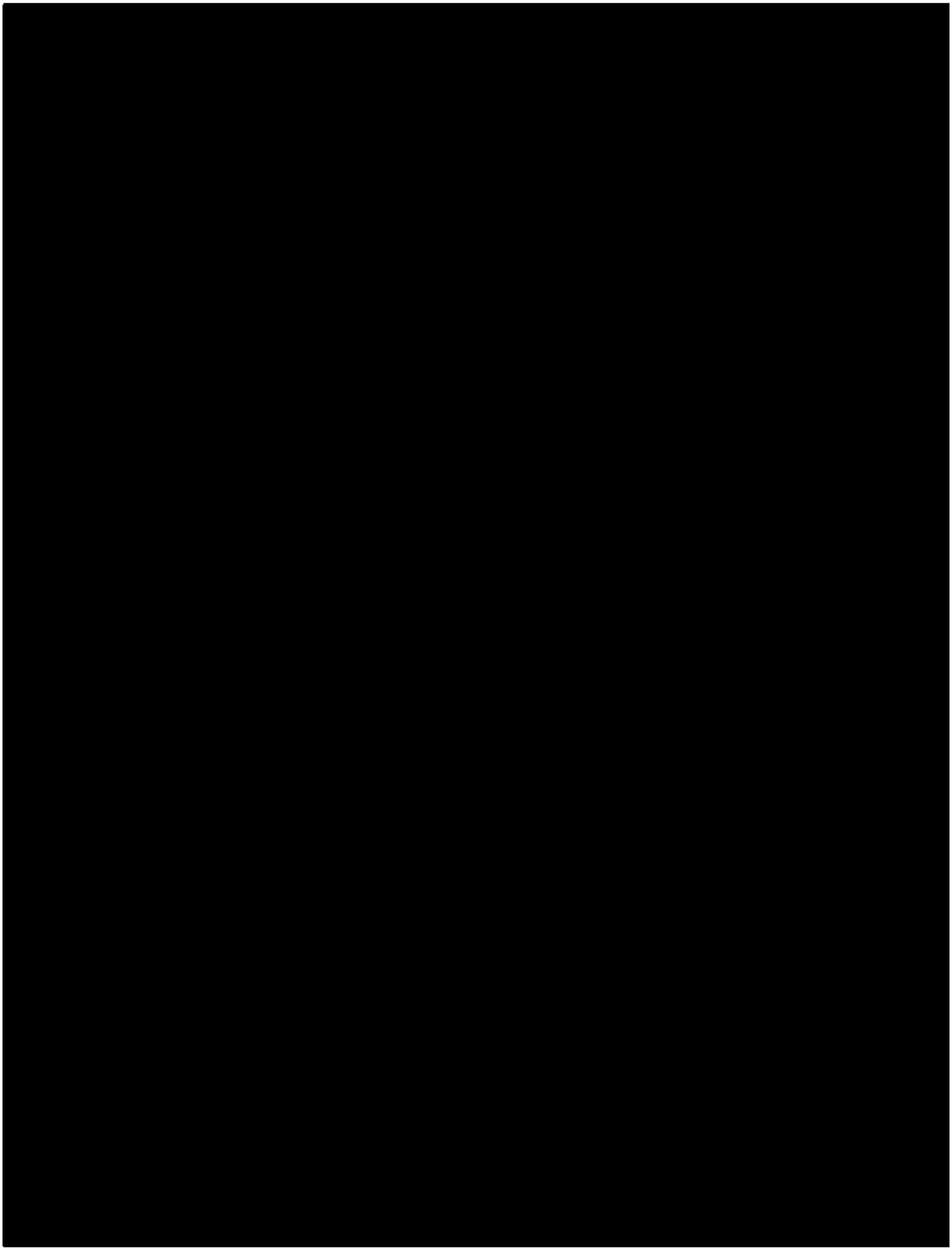
d. On or about April 1, 2019, Arslanian used WhatsApp to message Hana, writing, "You did not have one minute to text me on the way to the airport? It's Monday you promised the guy would come for the carpet. But I'm sure you'll be able to answer the phone about next Monday's meetings and dinner".

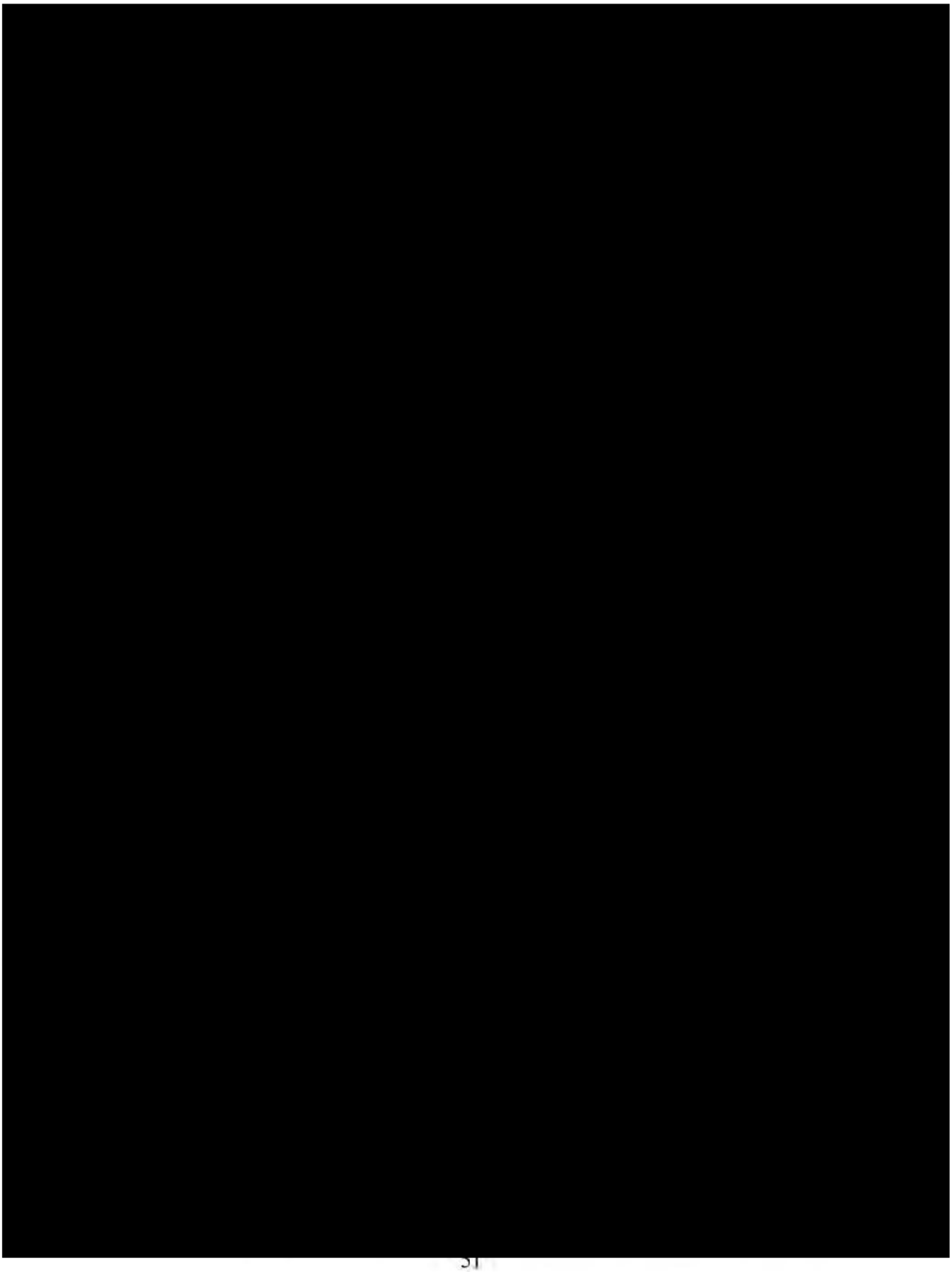
[redacted]











[redacted]

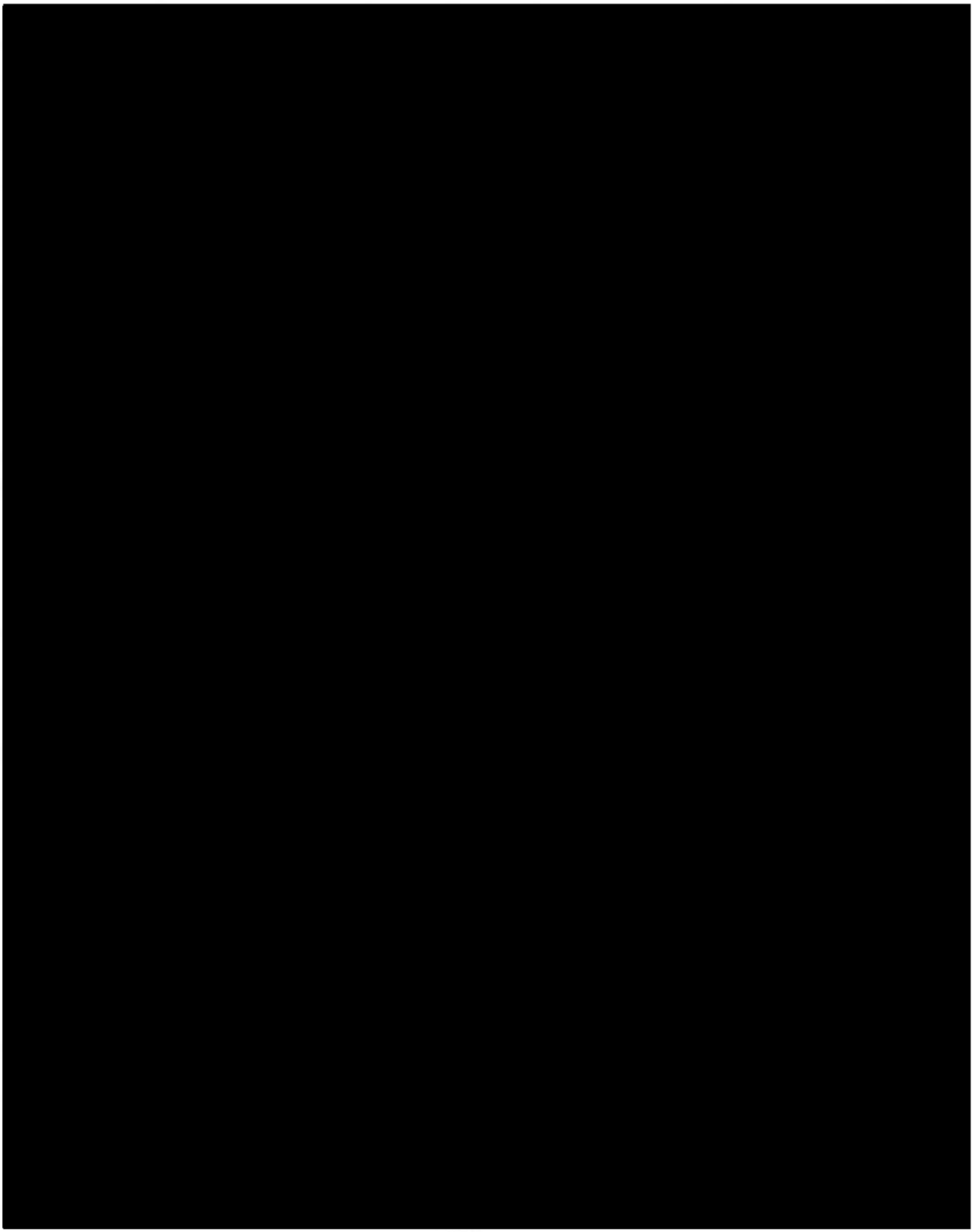
b. Based on my review of emails obtained from the search of the Arslanian Email Account, I have learned that, as of the date of the first preservation of that account (*i.e.*, approximately September 4, 2020), the majority of the emails that Subject Account-1 still contains with Arslanian (*i.e.*, approximately 25 of the 36 emails discussed above) appear to have been deleted from the Arslanian Email Account. As such, based on my training and experience, it appears that on some date prior to September 4, 2020, the user of the Arslanian Email Account (or someone with access to that account) deleted those 25 emails Arslanian had with Menendez that were sent from and/or to Subject Account-1. Further, as noted above, the Arslanian Email Account still contains spam emails received on the same date as emails that were deleted with Subject Account-1, and the Arslanian Email Account also still contains apparently personal emails with Menendez at Subject Account-1.[27] As such, based on my training and experience, and my review of emails more broadly in this investigation, I believe that emails with Subject Account-1 were selectively and intentionally deleted from the Arslanian Email Account, and that those emails that were deleted can still be found in Subject Account-1. Moreover, given that the Arslanian Email Account still contains emails with Menendez at Subject Account-1 that appear to be of a personal and facially non-incriminating nature, I believe that it is likely that the user of the Arslanian Email

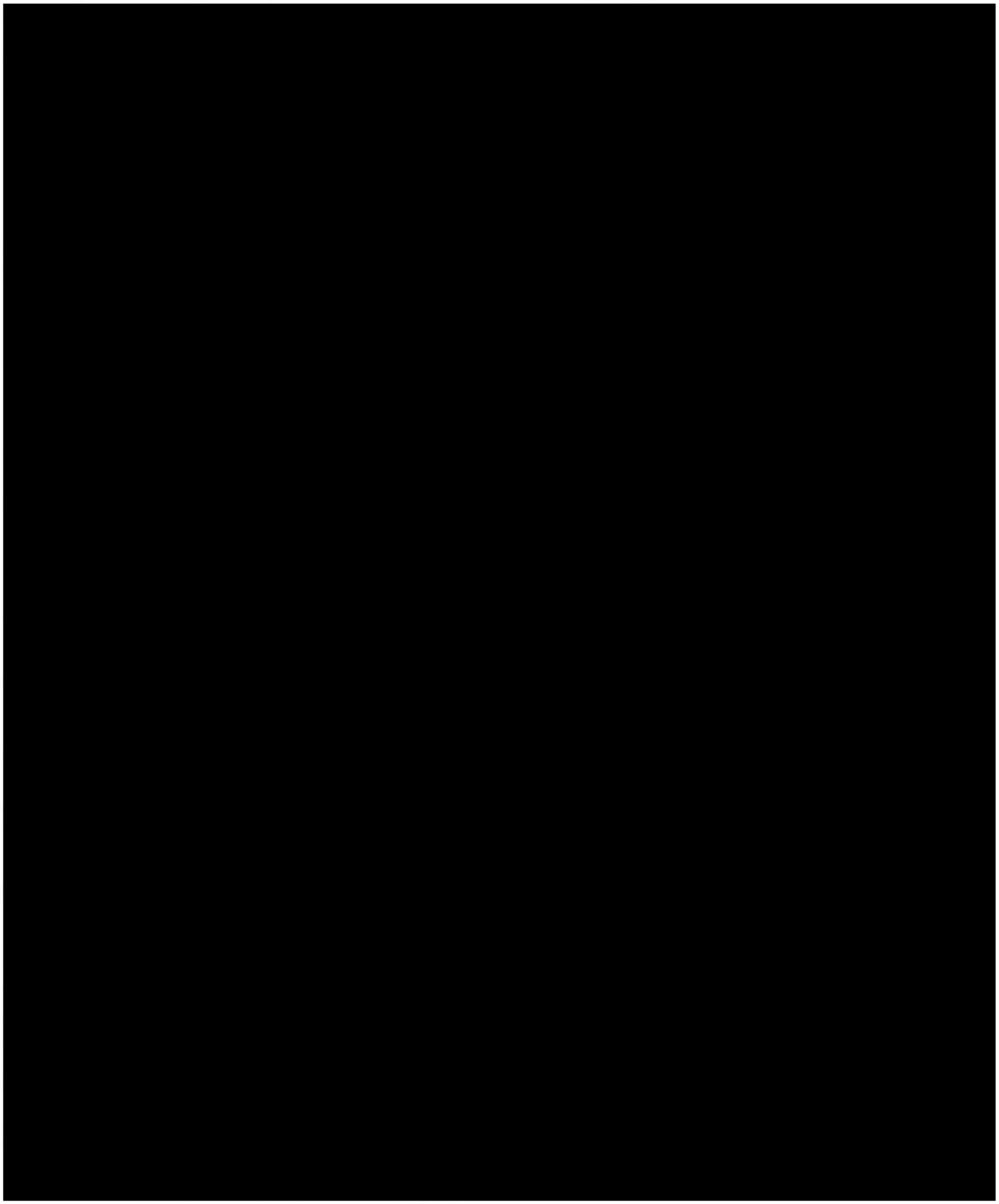
[27] Based on my review of the Arslanian Email Account, that email account still contains not only the 11 emails with Menendez that are still in Subject Account-1, but also contains different emails with Menendez of an apparently personal nature (which emails apparently have been deleted from Subject Account-1). Based on my training and experience, I believe that that strengthens the inference that the emails that were deleted from the Arslanian Email Account with Subject Account-1 were selectively deleted.

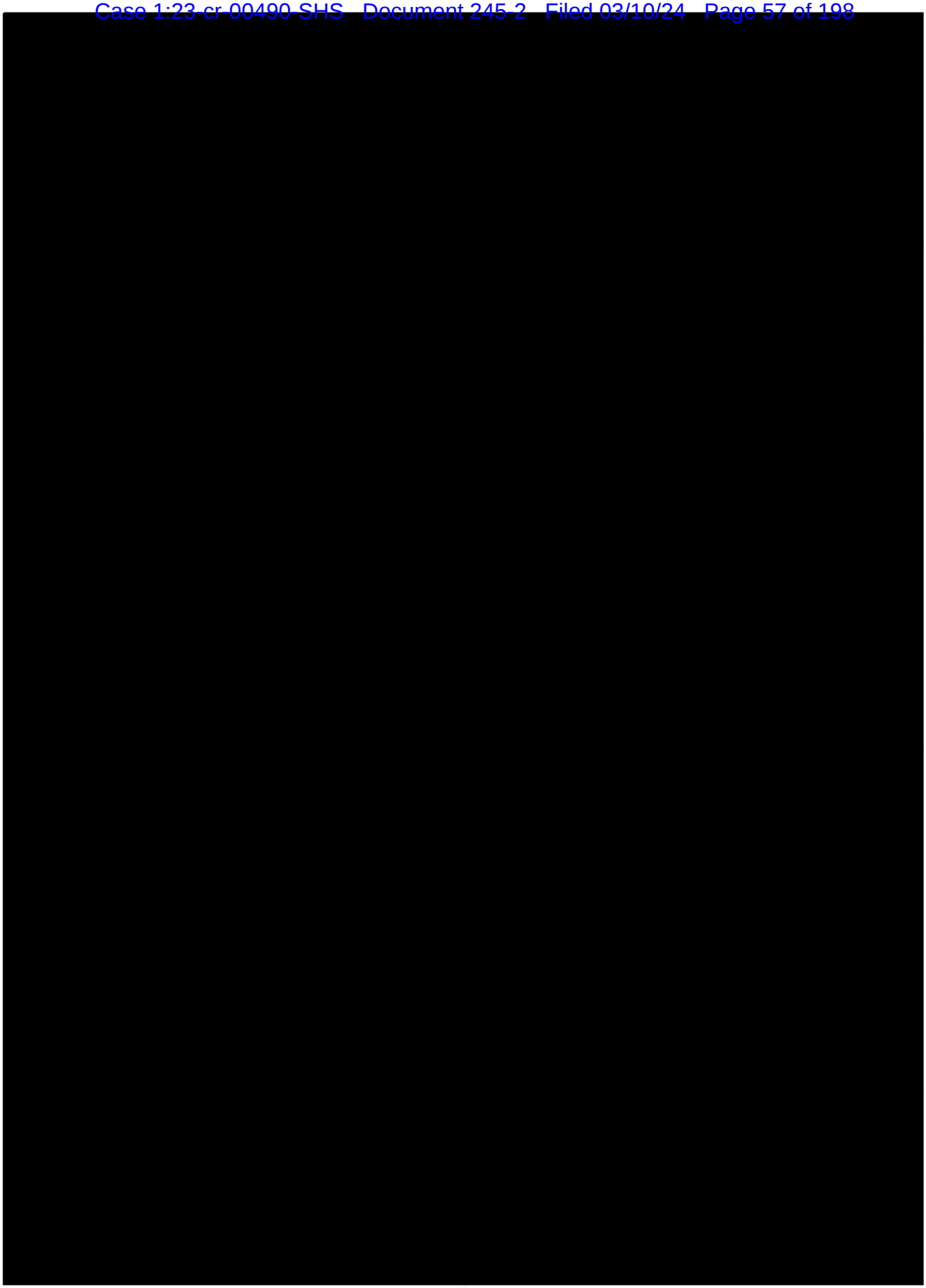
Account intentionally deleted other emails with Subject Account-1 (in particular, those that are still contained in Subject Account-1) in order to conceal them.

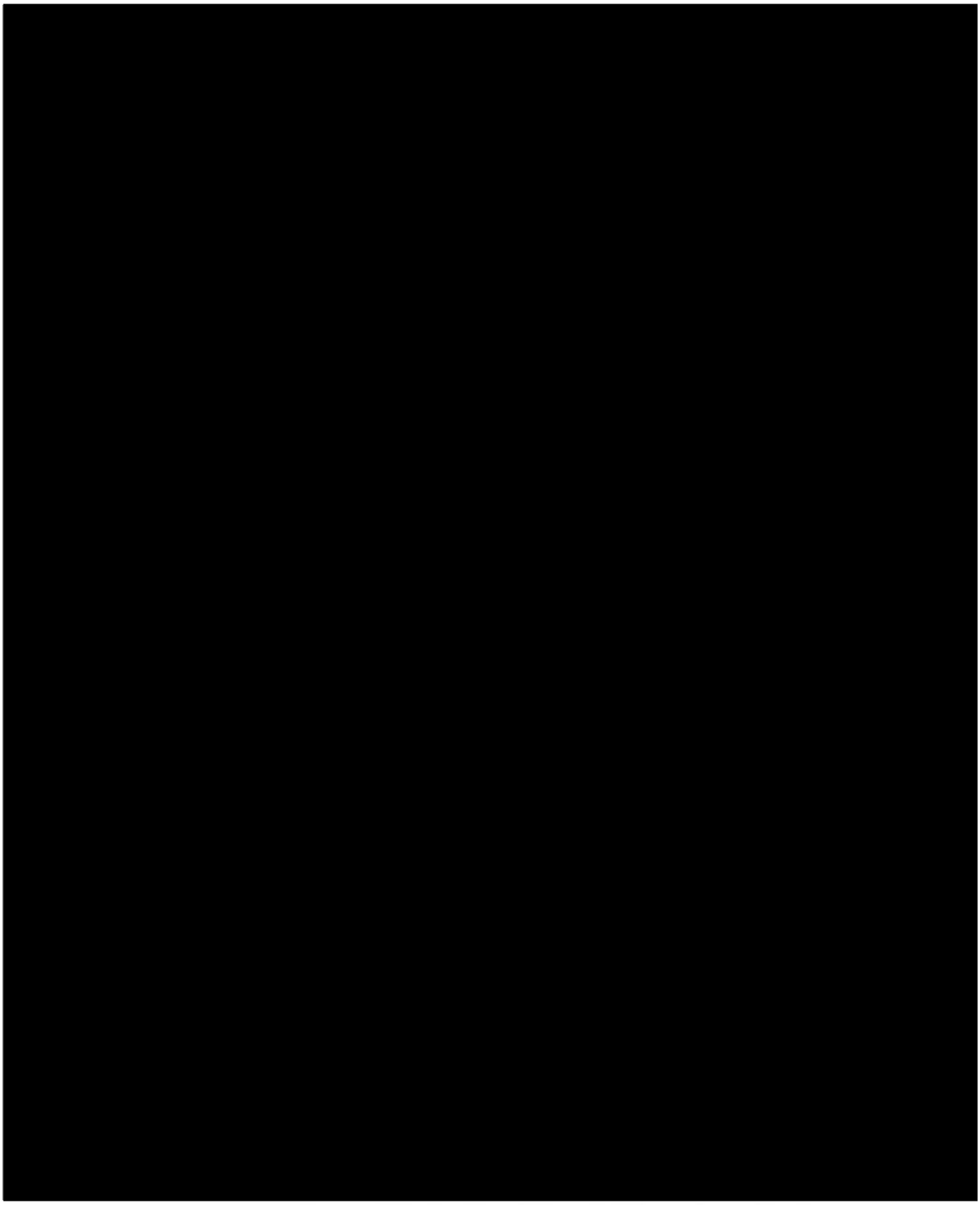
c. As discussed above, based on my training and experience, I believe that emails from the Second Hana Email Account, including those likely pertaining to the scheme, were likely intentionally and selectively deleted from the Arslanian Email Account (*see* paragraphs 41.b.ii, 41.d and footnote 18). As such, I believe this makes it more likely that emails with Subject Account-1 in the Arslanian Email Account were similarly intentionally and selectively deleted from the Arslanian Email Account and that those emails related to the scheme. In any event, it appears that approximately 25 emails between Menendez and Arslanian are still contained in Subject Account-1 and not in the Arslanian Email Account.

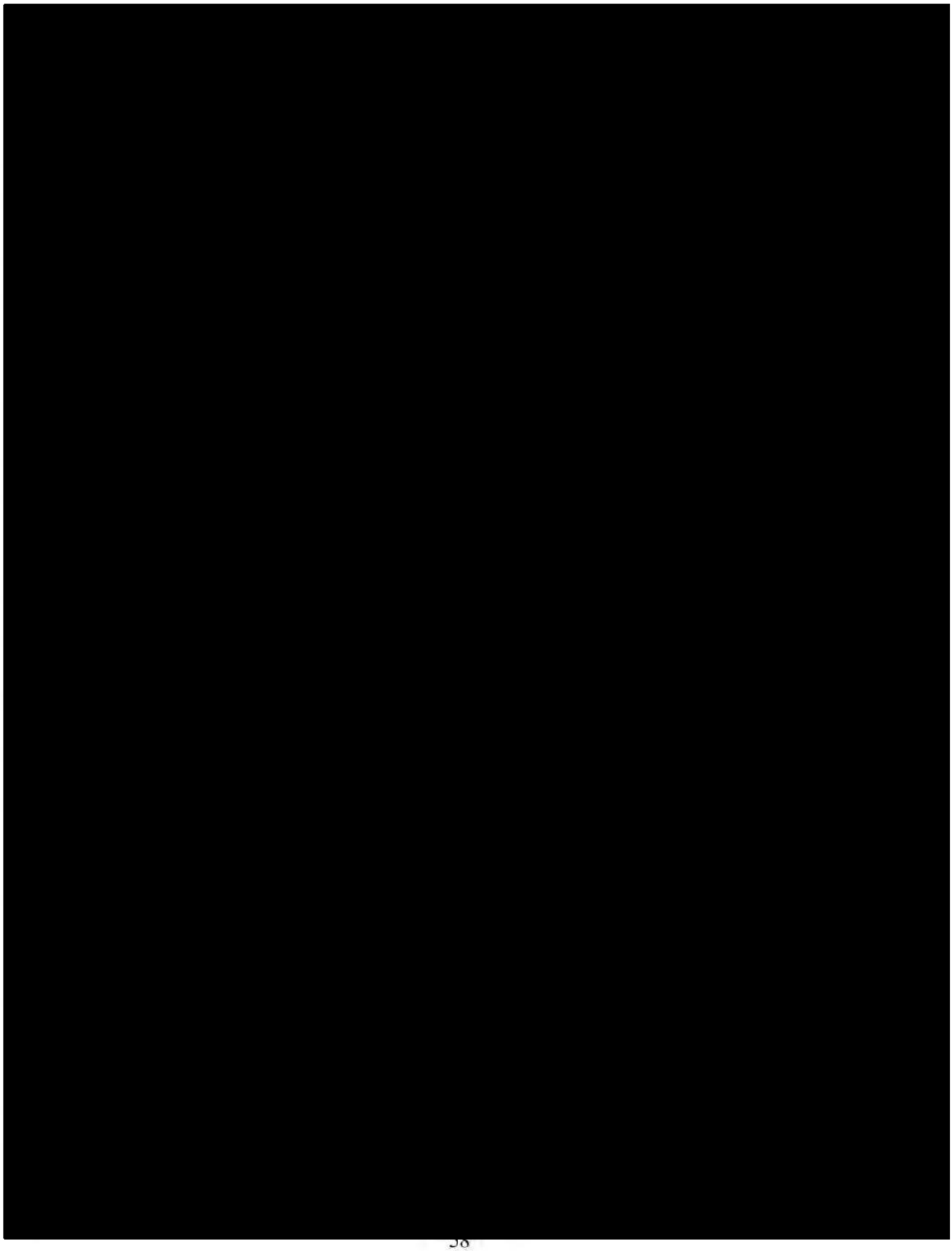
[redacted]

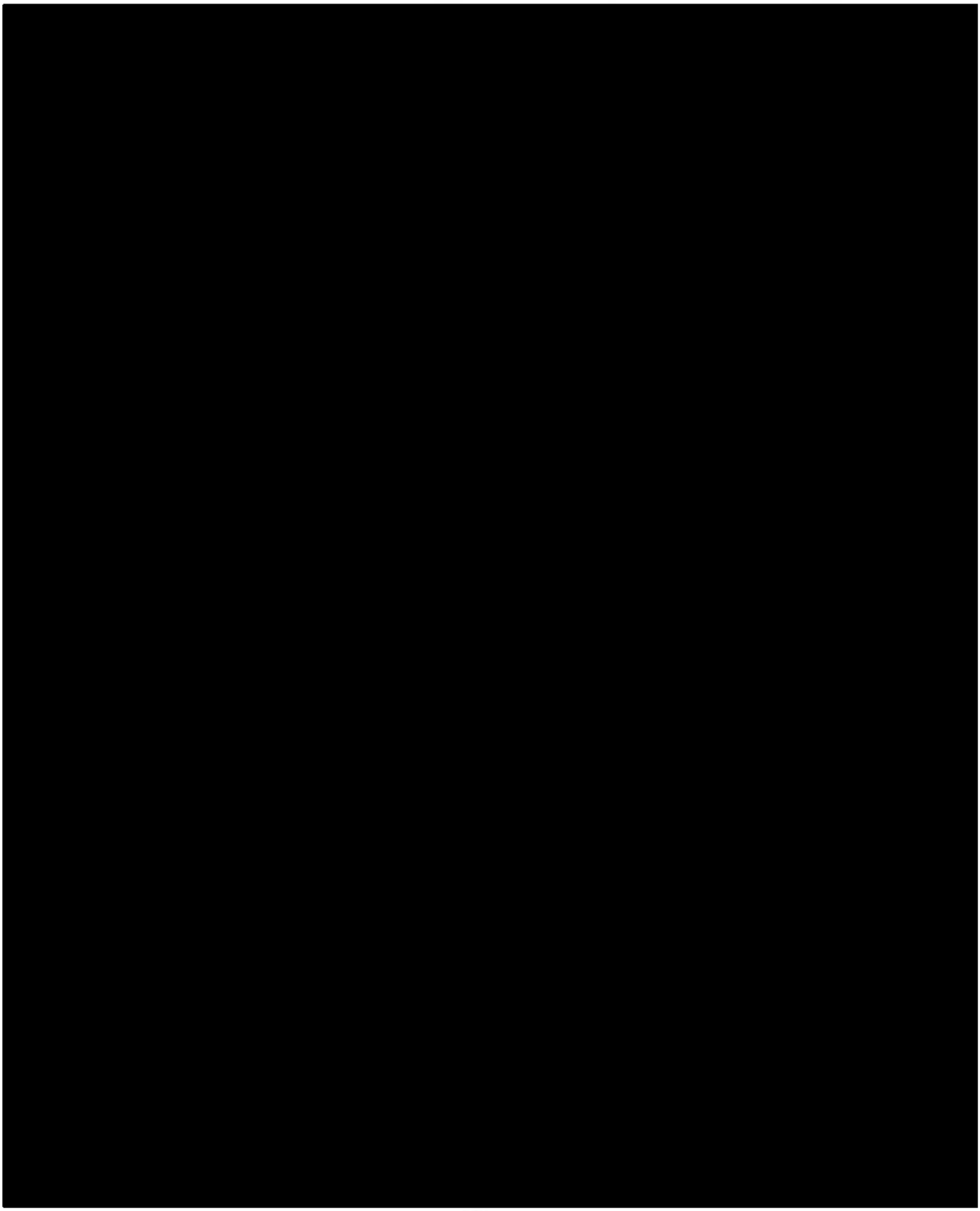


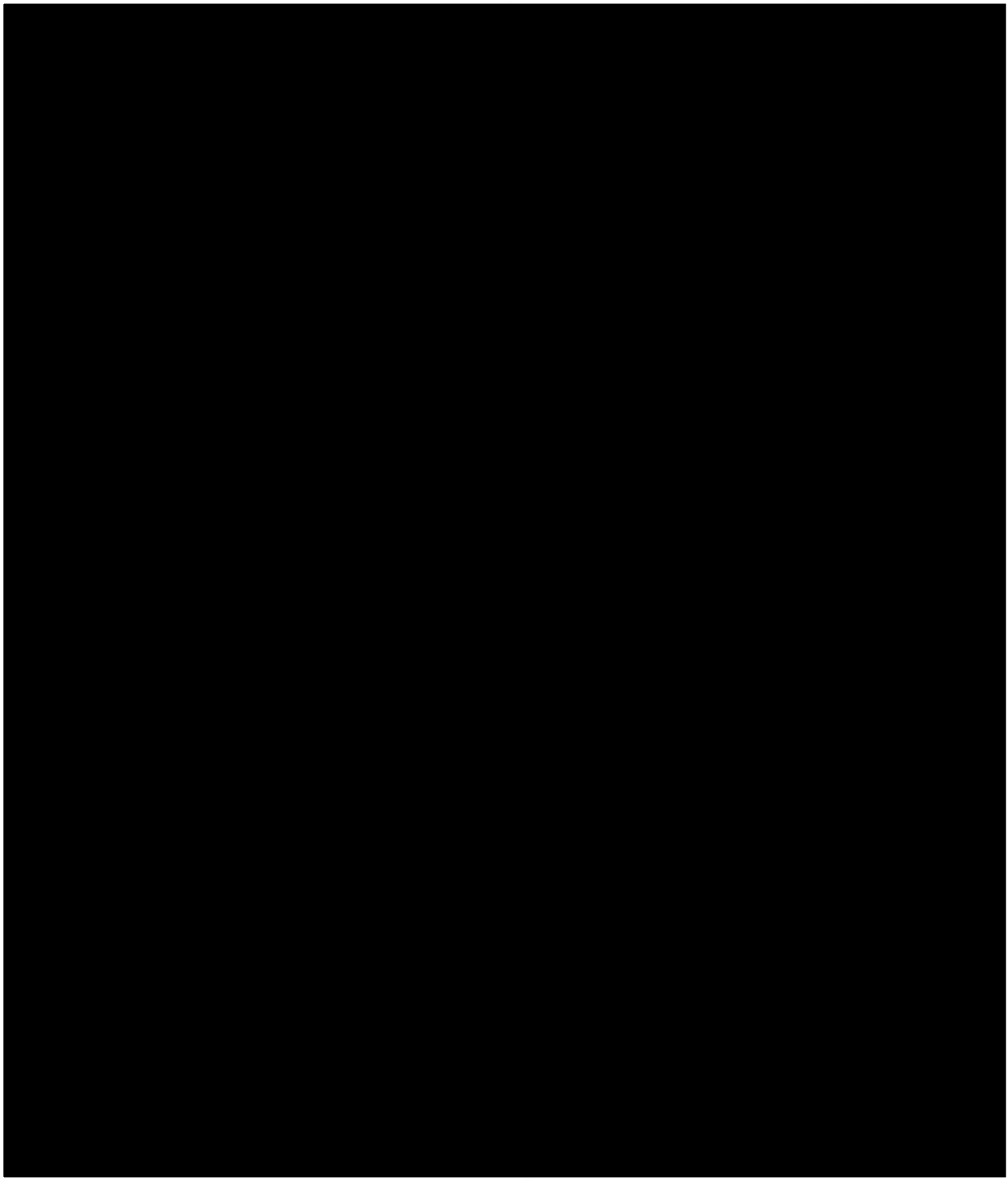


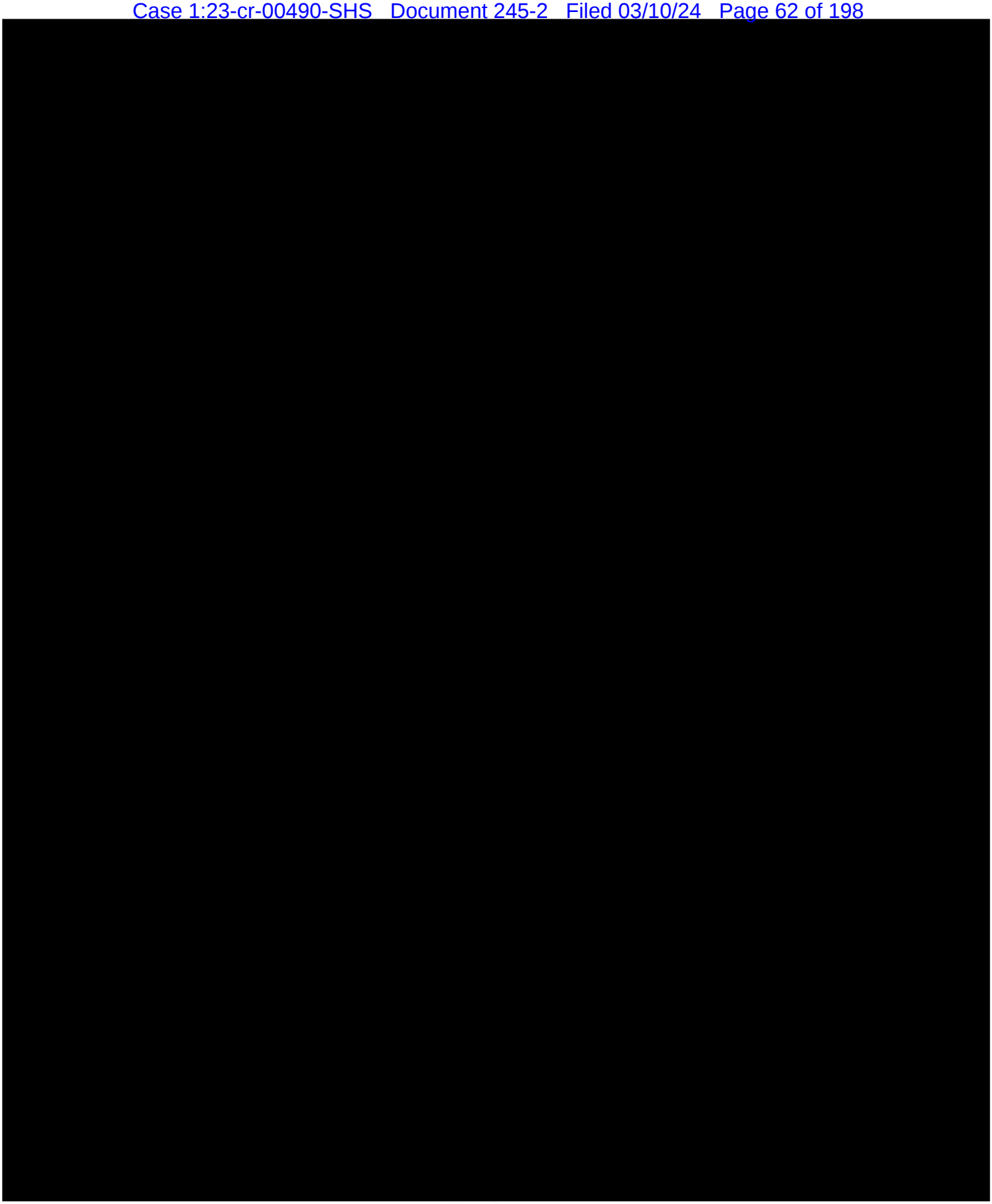


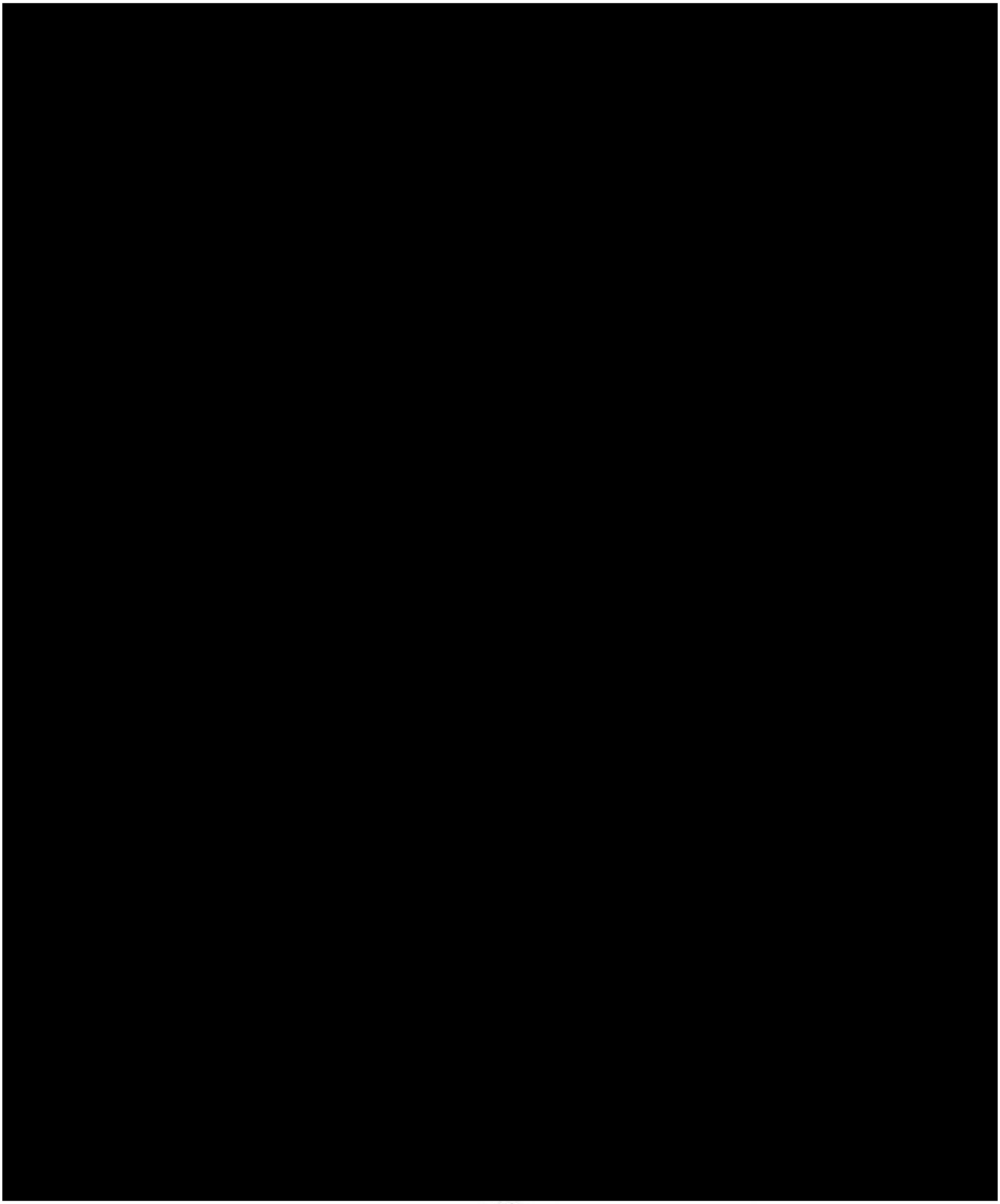












[redacted]

for.

58. Additionally, because Menendez may at times consult with attorneys or have other privileged communications, such as those potentially protected under the Speech or Debate Clause of Article One of the United States Constitution, the review of evidence seized from the Subject Accounts will be conducted pursuant to screening procedures to ensure that the law enforcement personnel involved in the investigation, including attorneys for the Government, collect evidence in a manner reasonably designed to protect any potential attorney-client or other applicable privilege. When appropriate, the procedures may include use of a designated "filter team," separate and apart from the investigative team, in order to review potentially privileged communications and determine which communications to release to the investigation and prosecution team, and/or production to Menendez's counsel for initial review and assertion of the Speech or Debate privilege potentially prior to any government review. As a result, in conducting this review, law enforcement personnel presently intend not to immediately commence review of the emails and/or other materials within the Subject Accounts, in order to ensure appropriate screening procedures are in place prior to review commencing, including potentially engaging with Menendez's counsel regarding such procedures once the investigation is overt as to him.

[redacted]